S01P0373

FIG. 1

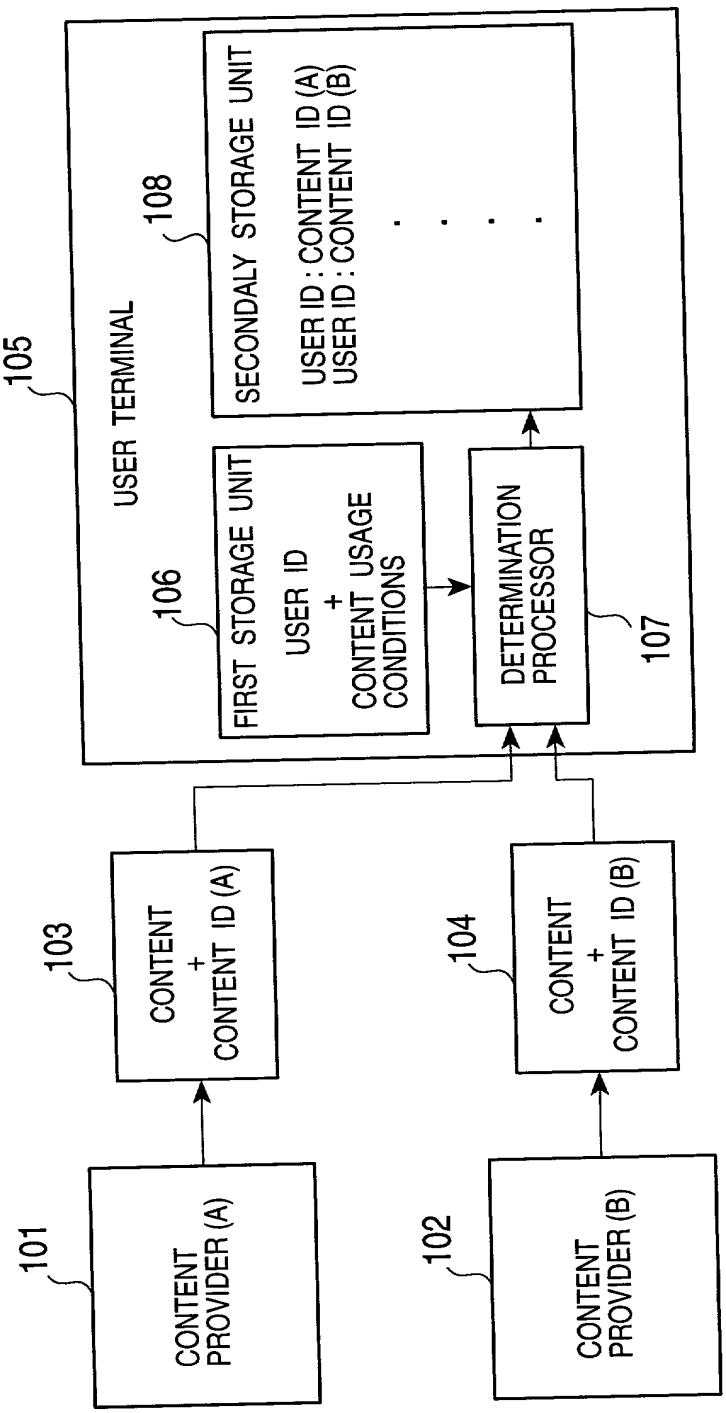


FIG. 2

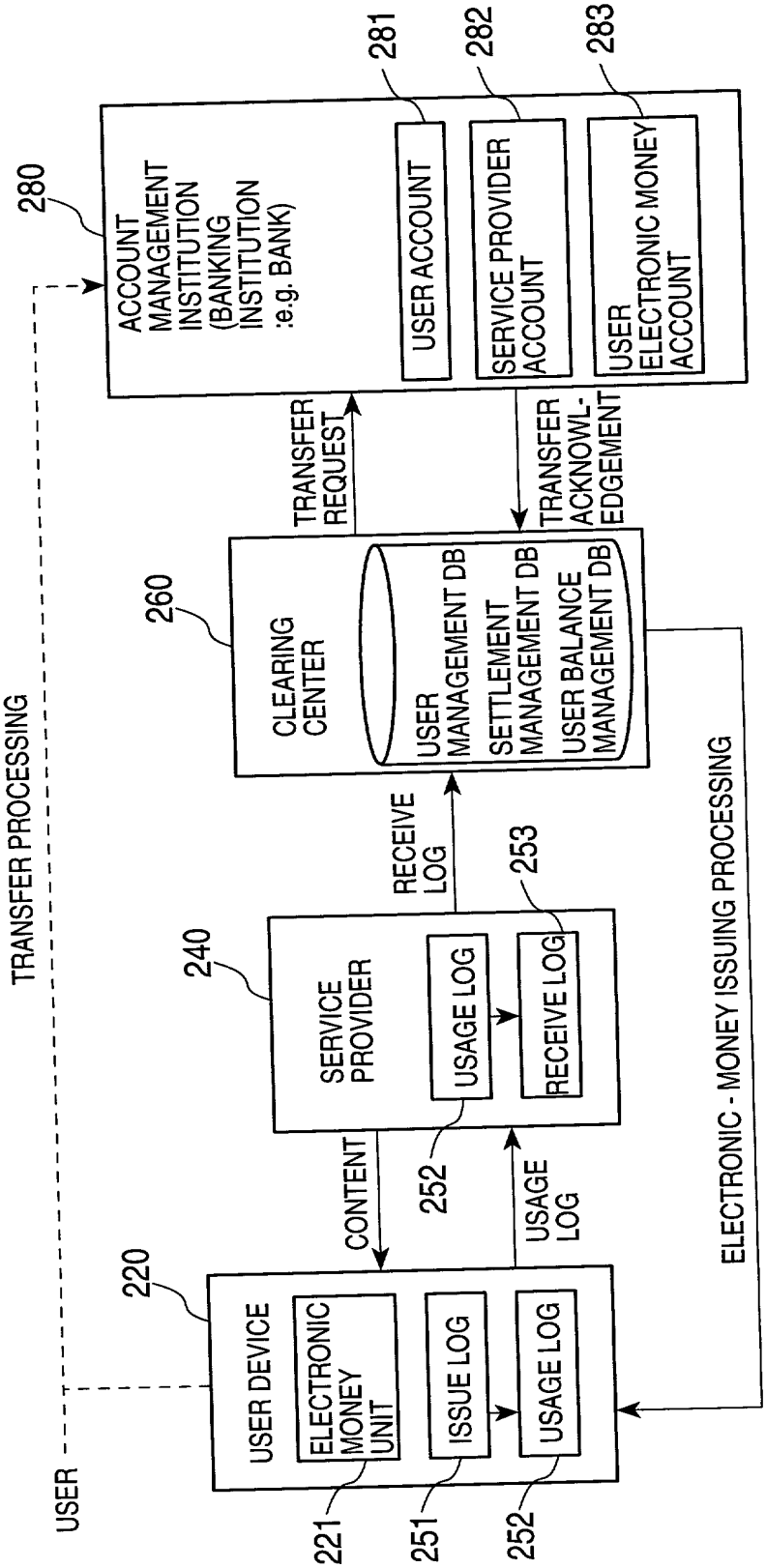

USER
TRANSFER PROCESSING
220
USER DEVICE
ELECTRONIC MONEY UNIT
ISSUE LOG
USAGE LOG
221
251
252
CONTENT
USAGE LOG
252
240
SERVICE PROVIDER
USAGE LOG
RECEIVE LOG
253
RECEIVE LOG
260
CLEARING CENTER
USER MANAGEMENT DB
SETTLEMENT MANAGEMENT DB
USER BALANCE MANAGEMENT DB
TRANSFER REQUEST
TRANSFER ACKNOWL-EDGEMENT
ELECTRONIC - MONEY ISSUING PROCESSING
280
ACCOUNT MANAGEMENT INSTITUTION (BANKING INSTITUTION :e.g. BANK)
281
USER ACCOUNT
282
SERVICE PROVIDER ACCOUNT
283
USER ELECTRONIC MONEY ACCOUNT

FIG. 3

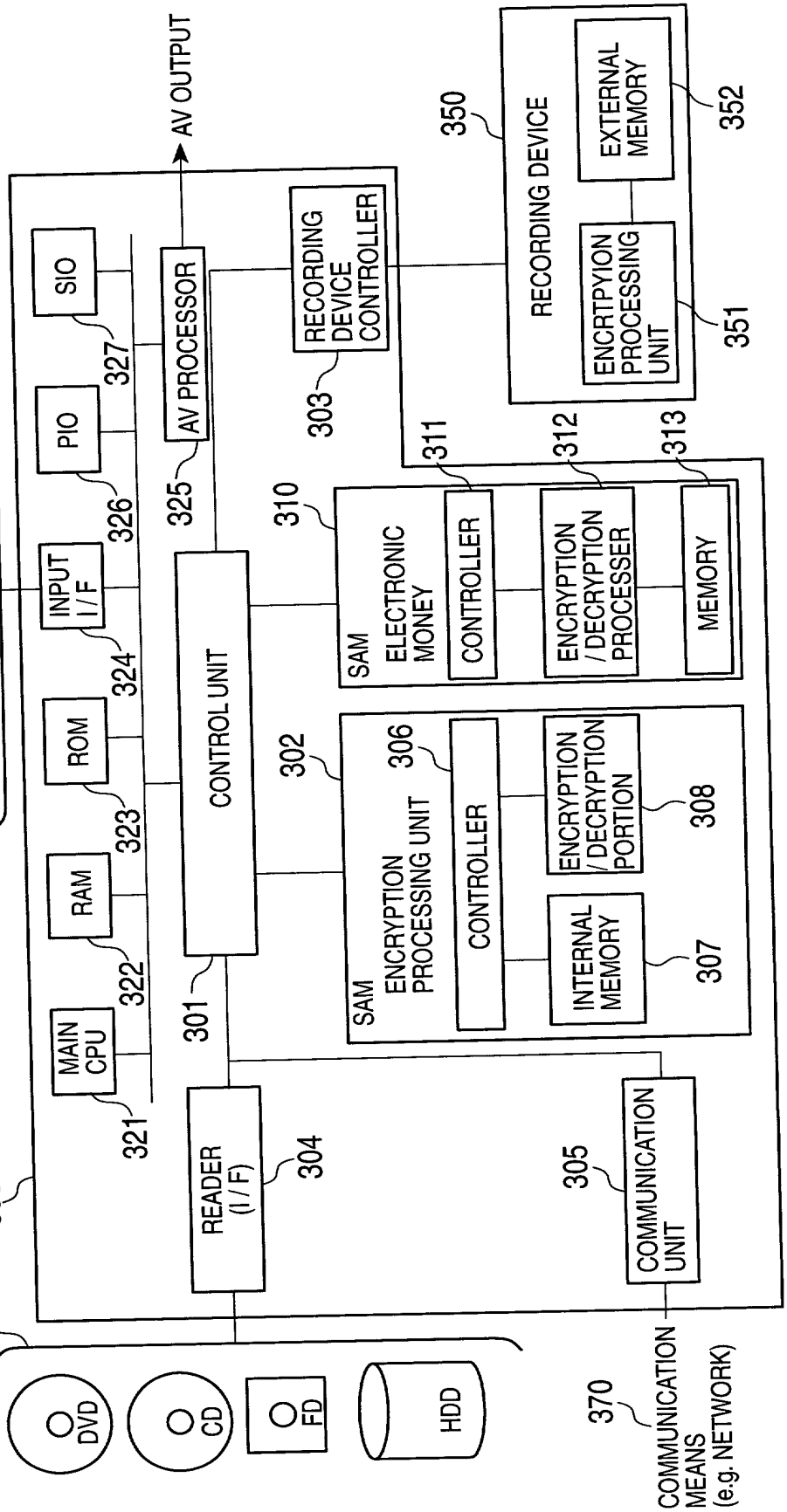

CONTROLLER
KEYBOARD
MOUSE
AV OUTPUT
SIO
PIO
INPUT I/F
ROM
RAM
MAIN CPU
CONTROL UNIT
AV PROCESSOR
RECORDING DEVICE CONTROLLER
RECORDING DEVICE
EXTERNAL MEMORY
ENCRTPYION PROCESSING UNIT
SAM
ELECTRONIC MONEY
CONTROLLER
ENCRYPTION /DECRYPTION PROCESSER
MEMORY
SAM
ENCRYPTION PROCESSING UNIT
CONTROLLER
ENCRYPTION /DECRYPTION PORTION
INTERNAL MEMORY
READER (I/F)
COMMUNICATION UNIT
DVD
CD
FD
HDD
COMMUNICATION MEANS (e.g. NETWORK)
300
301
302
303
304
305
306
307
308
310
311
312
313
321
322
323
324
325
326
327
350
351
352
360
370

FIG. 4

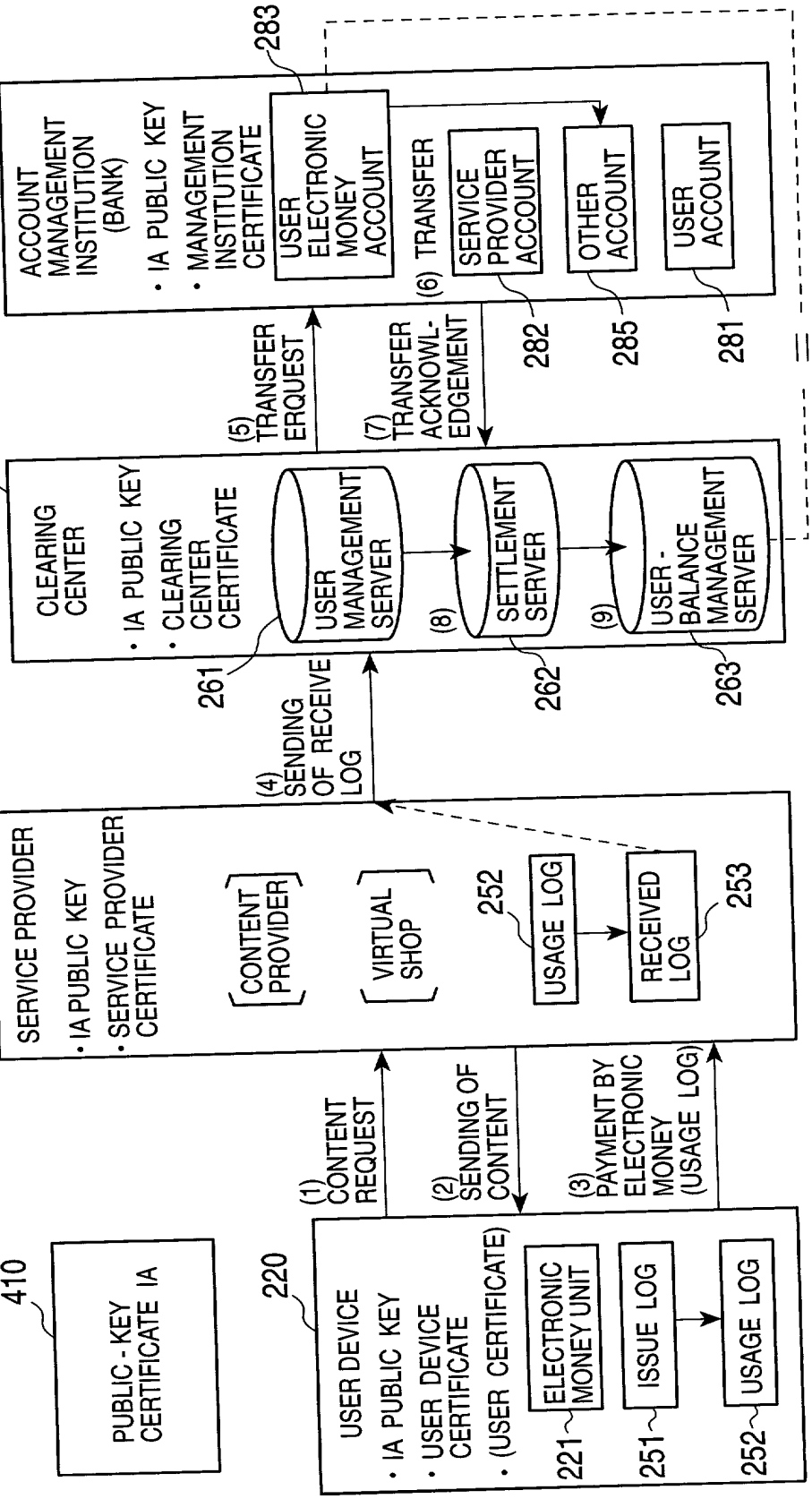

410
PUBLIC - KEY CERTIFICATE IA
220
USER DEVICE
• IA PUBLIC KEY
• USER DEVICE CERTIFICATE
• (USER CERTIFICATE)
221 ELECTRONIC MONEY UNIT
251 ISSUE LOG
252 USAGE LOG
(1) CONTENT REQUEST
(2) SENDING OF CONTENT
(3) PAYMENT BY ELECTRONIC MONEY (USAGE LOG)
240
SERVICE PROVIDER
• IA PUBLIC KEY
• SERVICE PROVIDER CERTIFICATE
CONTENT PROVIDER
VIRTUAL SHOP
252 USAGE LOG
253 RECEIVED LOG
(4) SENDING OF RECEIVE LOG
260
CLEARING CENTER
• IA PUBLIC KEY
• CLEARING CENTER CERTIFICATE
261 USER MANAGEMENT SERVER
(8)
262 SETTLEMENT SERVER
(9)
263 USER - BALANCE MANAGEMENT SERVER
(5) TRANSFER ERQUEST
(7) TRANSFER ACKNOWL-EDGEMENT
280
ACCOUNT MANAGEMENT INSTITUTION (BANK)
• IA PUBLIC KEY
• MANAGEMENT INSTITUTION CERTIFICATE
283 USER ELECTRONIC MONEY ACCOUNT
(6) TRANSFER
282 SERVICE PROVIDER ACCOUNT
285 OTHER ACCOUNT
281 USER ACCOUNT

FIG. 5

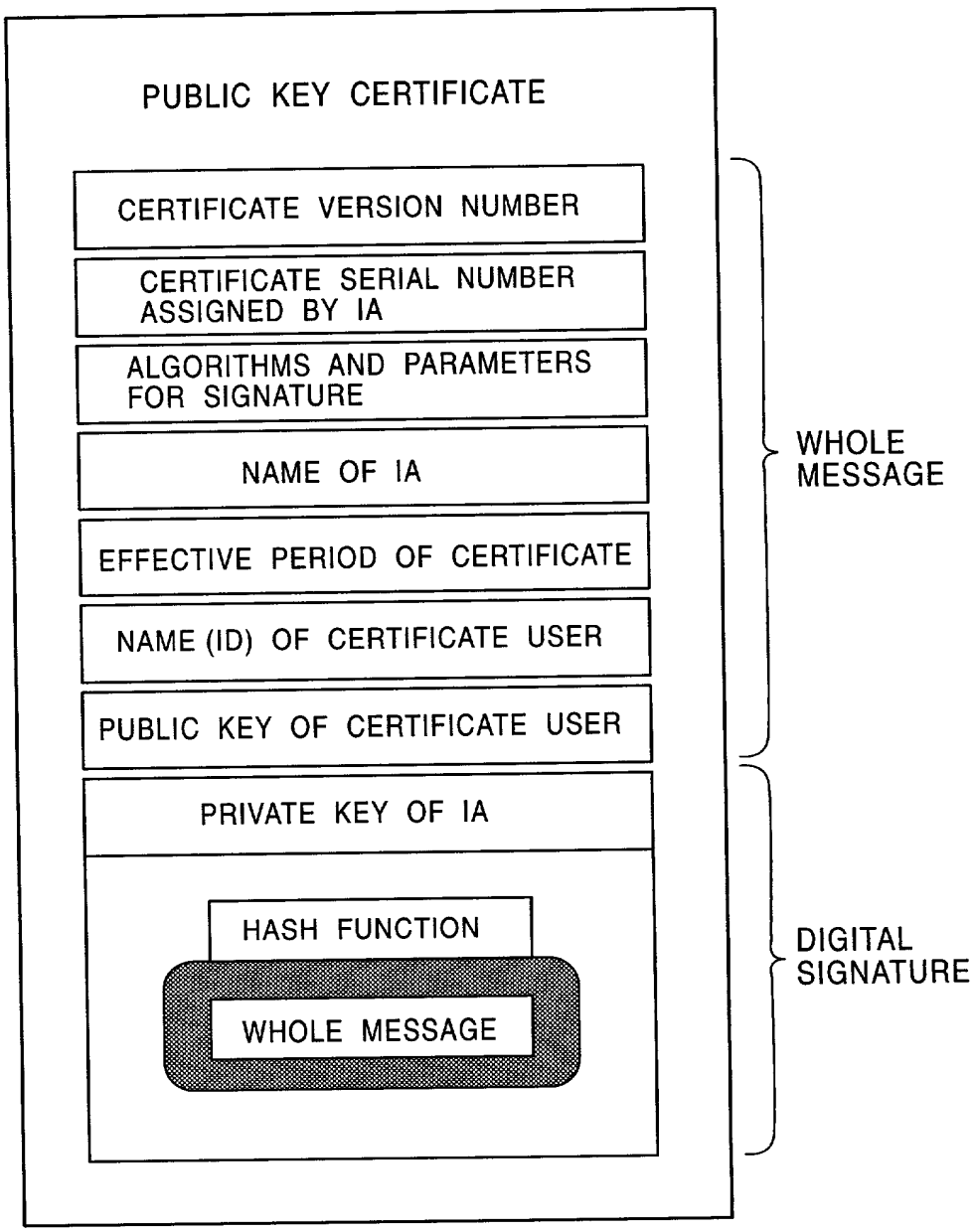

PUBLIC KEY CERTIFICATE
CERTIFICATE VERSION NUMBER
CERTIFICATE SERIAL NUMBER ASSIGNED BY IA
ALGORITHMS AND PARAMETERS FOR SIGNATURE
NAME OF IA
EFFECTIVE PERIOD OF CERTIFICATE
NAME (ID) OF CERTIFICATE USER
PUBLIC KEY OF CERTIFICATE USER
PRIVATE KEY OF IA
HASH FUNCTION
WHOLE MESSAGE
WHOLE MESSAGE
DIGITAL SIGNATURE

FIG. 6

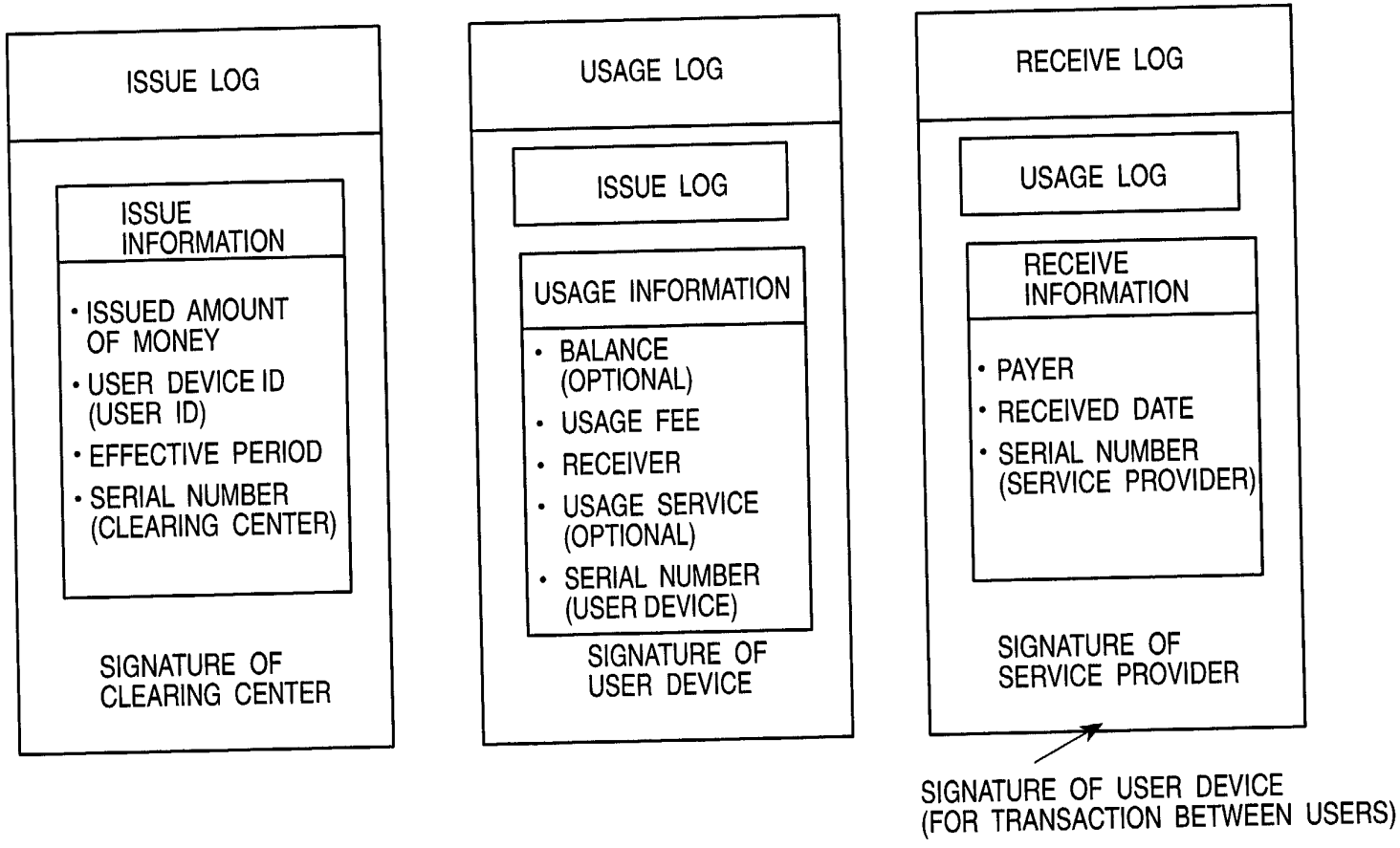

ISSUE LOG
ISSUE INFORMATION
• ISSUED AMOUNT OF MONEY
• USER DEVICE ID (USER ID)
• EFFECTIVE PERIOD
• SERIAL NUMBER (CLEARING CENTER)
SIGNATURE OF CLEARING CENTER
USAGE LOG
ISSUE LOG
USAGE INFORMATION
• BALANCE (OPTIONAL)
• USAGE FEE
• RECEIVER
• USAGE SERVICE (OPTIONAL)
• SERIAL NUMBER (USER DEVICE)
SIGNATURE OF USER DEVICE
RECEIVE LOG
USAGE LOG
RECEIVE INFORMATION
• PAYER
• RECEIVED DATE
• SERIAL NUMBER (SERVICE PROVIDER)
SIGNATURE OF SERVICE PROVIDER
SIGNATURE OF USER DEVICE (FOR TRANSACTION BETWEEN USERS)

FIG. 7

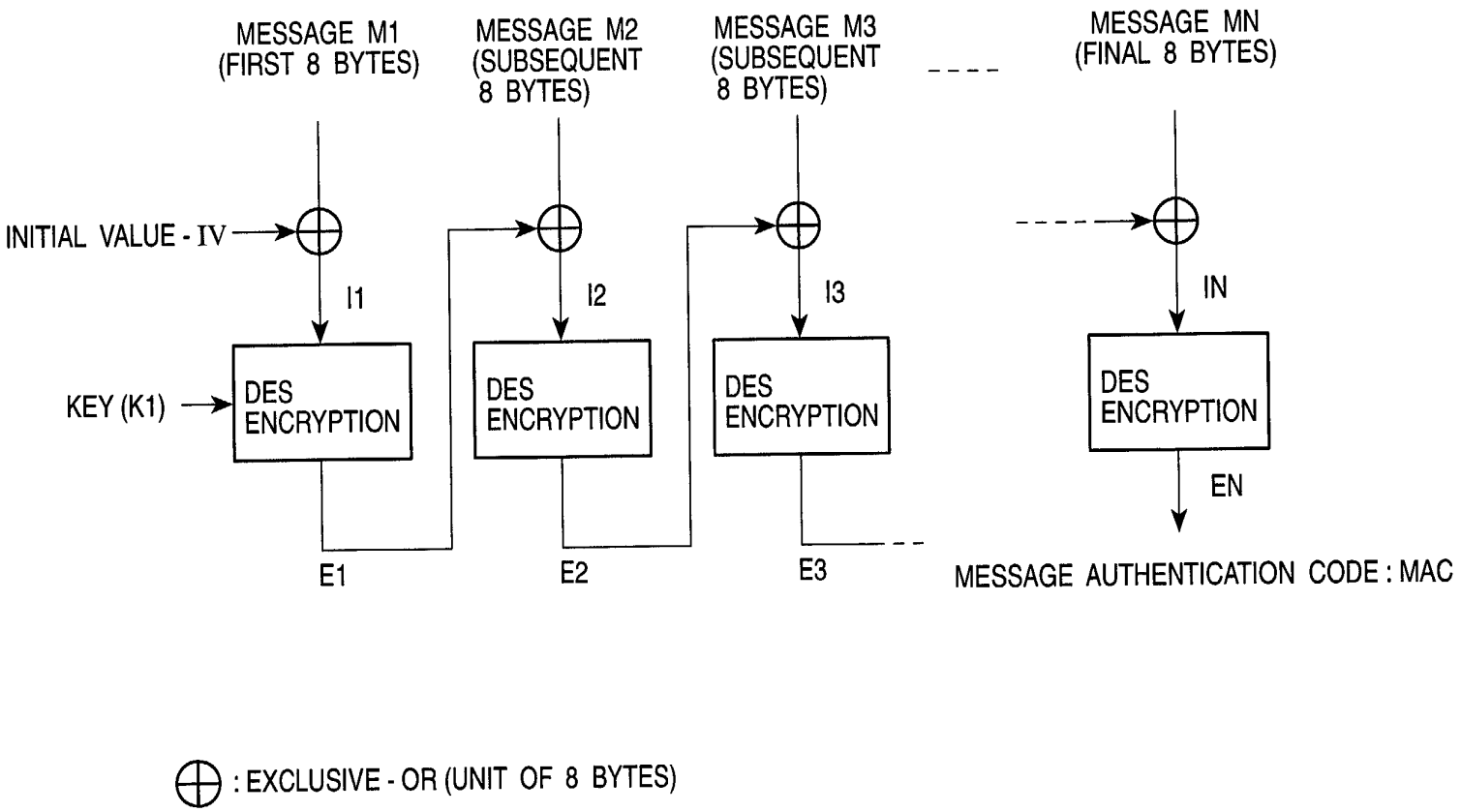

MESSAGE M1
(FIRST 8 BYTES)
MESSAGE M2
(SUBSEQUENT
8 BYTES)
MESSAGE M3
(SUBSEQUENT
8 BYTES)
MESSAGE MN
(FINAL 8 BYTES)
INITIAL VALUE - IV
I1
I2
I3
IN
KEY (K1)
DES
ENCRYPTION
DES
ENCRYPTION
DES
ENCRYPTION
DES
ENCRYPTION
EN
E1
E2
E3
MESSAGE AUTHENTICATION CODE : MAC
⊕ : EXCLUSIVE - OR (UNIT OF 8 BYTES)

FIG. 8

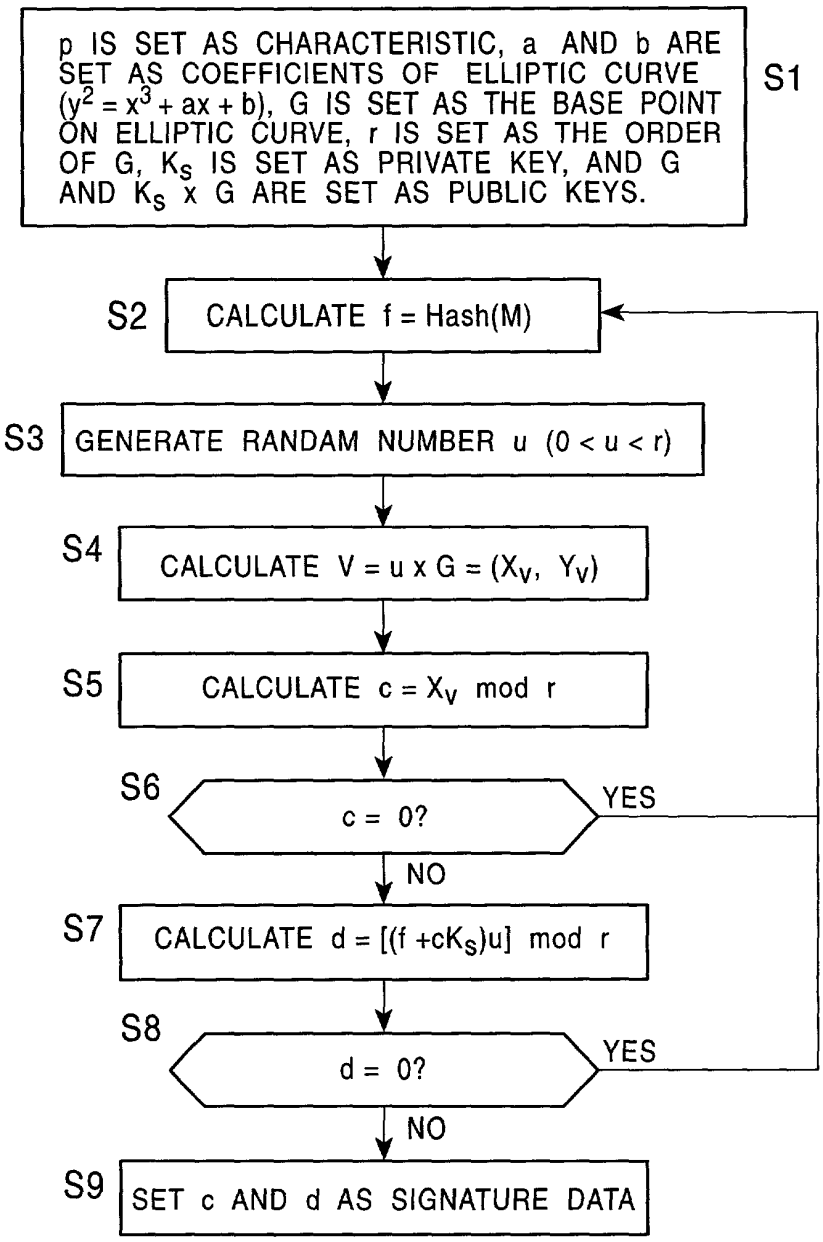

p IS SET AS CHARACTERISTIC, a AND b ARE SET AS COEFFICIENTS OF ELLIPTIC CURVE ($y^2 = x^3 + ax + b$), G IS SET AS THE BASE POINT ON ELLIPTIC CURVE, r IS SET AS THE ORDER OF G, K_S IS SET AS PRIVATE KEY, AND G AND K_S x G ARE SET AS PUBLIC KEYS.
S1
S2
CALCULATE f = Hash(M)
S3
GENERATE RANDAM NUMBER u (0 < u < r)
S4
CALCULATE V = u x G = (X_V, Y_V)
S5
CALCULATE c = X_V mod r
S6
c = 0?
YES
NO
S7
CALCULATE d = [(f +cK_S)u] mod r
S8
d = 0?
YES
NO
S9
SET c AND d AS SIGNATURE DATA

FIG. 9

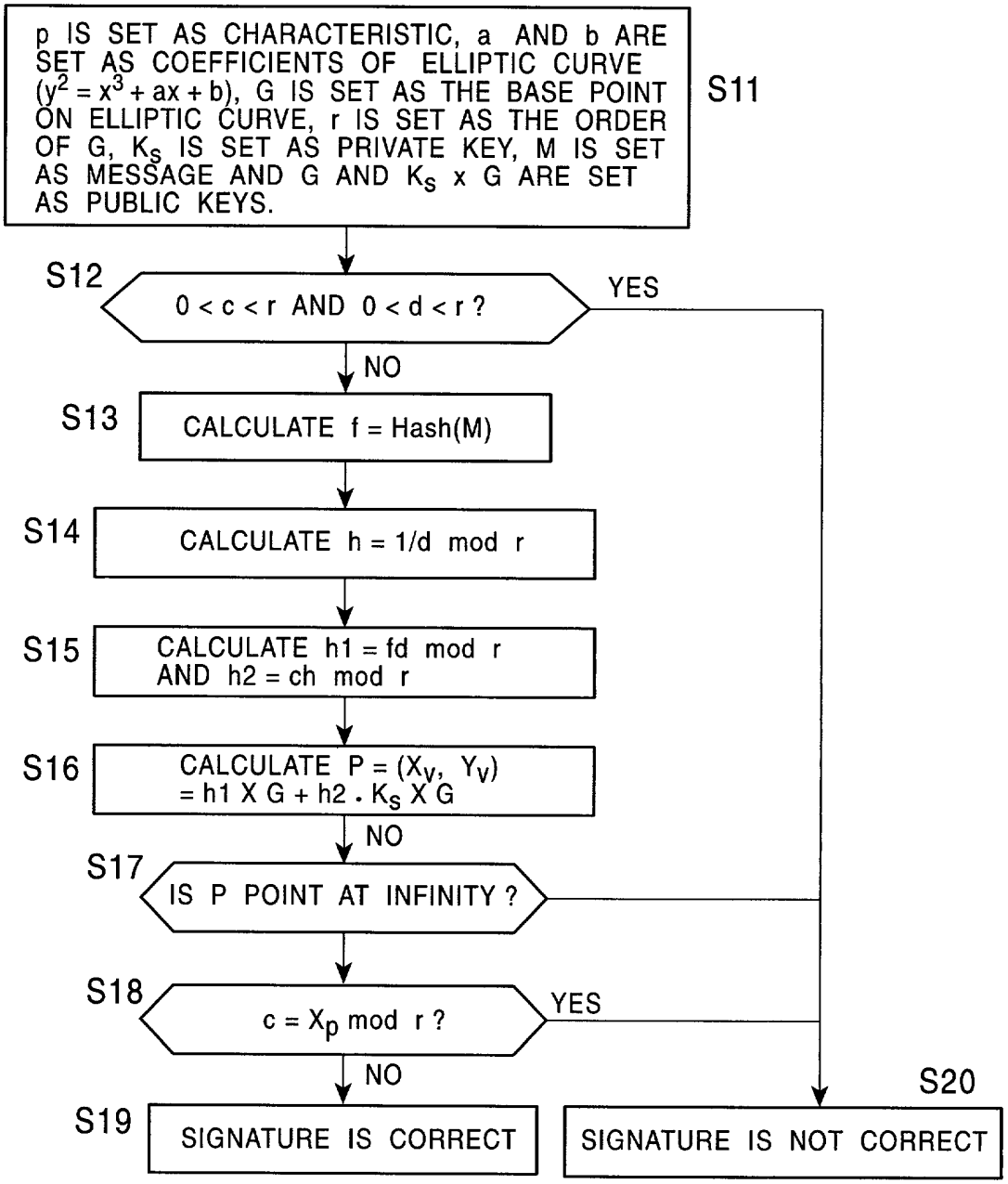

p IS SET AS CHARACTERISTIC, a AND b ARE SET AS COEFFICIENTS OF ELLIPTIC CURVE ($y^2 = x^3 + ax + b$), G IS SET AS THE BASE POINT ON ELLIPTIC CURVE, r IS SET AS THE ORDER OF G, K_S IS SET AS PRIVATE KEY, M IS SET AS MESSAGE AND G AND K_S x G ARE SET AS PUBLIC KEYS.
S11
S12
0 < c < r AND 0 < d < r ?
YES
NO
S13
CALCULATE f = Hash(M)
S14
CALCULATE h = 1/d mod r
S15
CALCULATE h1 = fd mod r AND h2 = ch mod r
S16
CALCULATE P = (X_V, Y_V) = h1 X G + h2 . K_S X G
NO
S17
IS P POINT AT INFINITY ?
S18
c = X_p mod r ?
YES
NO
S19
SIGNATURE IS CORRECT
S20
SIGNATURE IS NOT CORRECT

FIG. 10

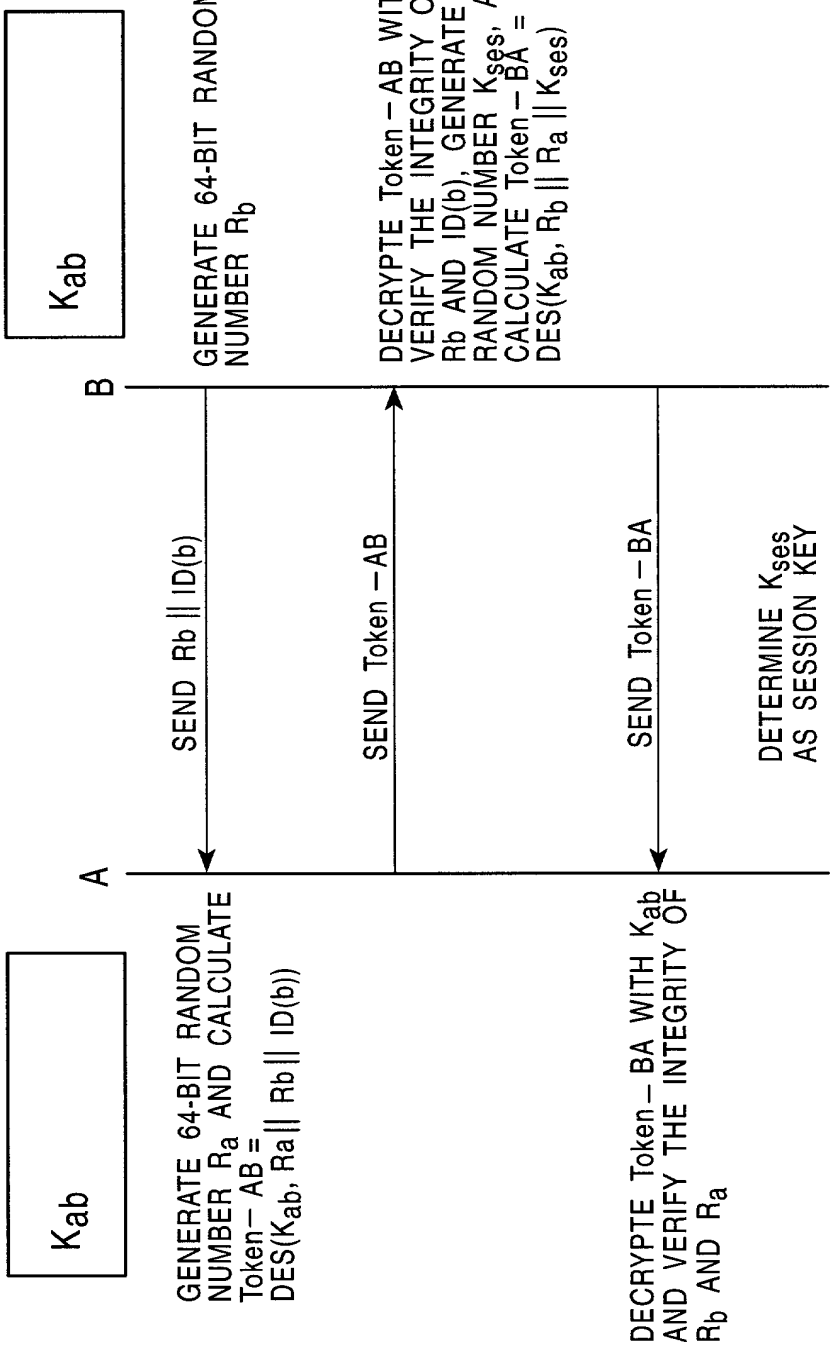

A
B
K_{ab}
K_{ab}
GENERATE 64-BIT RANDOM NUMBER R_a AND CALCULATE Token−AB = DES(K_{ab}, Ra || Rb || ID(b))
SEND Rb || ID(b)
GENERATE 64-BIT RANDOM NUMBER R_b
DECRYPTE Token−AB WITH K_{ab}, VERIFY THE INTEGRITY OF Rb AND ID(b), GENERATE 64-BIT RANDOM NUMBER K_{ses}, AND CALCULATE Token−BA = DES(K_{ab}, R_b || R_a || K_{ses})
SEND Token−AB
SEND Token−BA
DECRYPTE Token−BA WITH K_{ab} AND VERIFY THE INTEGRITY OF R_b AND R_a
DETERMINE K_{ses} AS SESSION KEY

FIG. 11

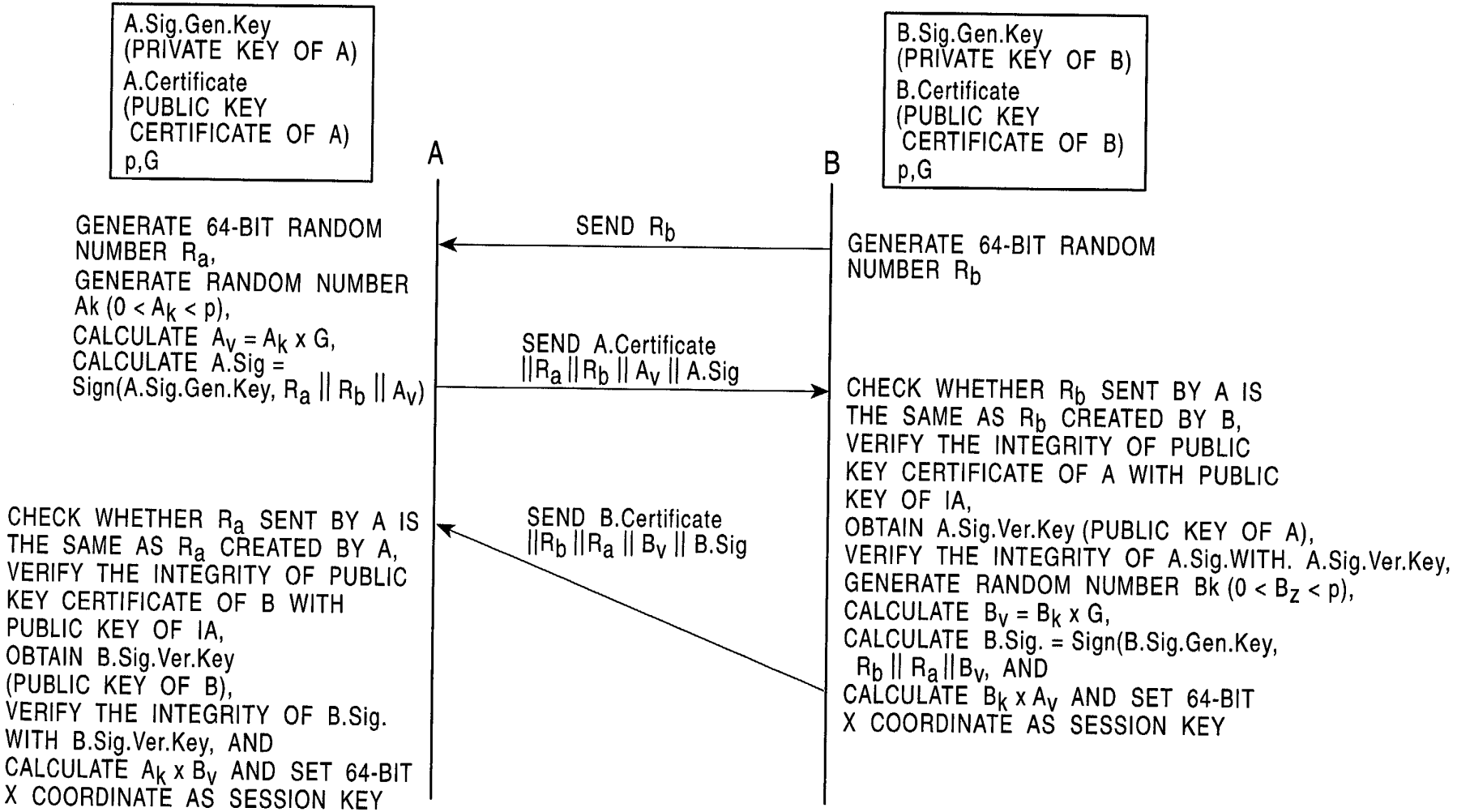

A.Sig.Gen.Key
(PRIVATE KEY OF A)
A.Certificate
(PUBLIC KEY
CERTIFICATE OF A)
p,G
B.Sig.Gen.Key
(PRIVATE KEY OF B)
B.Certificate
(PUBLIC KEY
CERTIFICATE OF B)
p,G
A
B
GENERATE 64-BIT RANDOM NUMBER Ra,
GENERATE RANDOM NUMBER Ak (0 < Ak < p),
CALCULATE Av = Ak x G,
CALCULATE A.Sig = Sign(A.Sig.Gen.Key, Ra || Rb || Av)
SEND Rb
GENERATE 64-BIT RANDOM NUMBER Rb
SEND A.Certificate ||Ra||Rb || Av || A.Sig
CHECK WHETHER Rb SENT BY A IS THE SAME AS Rb CREATED BY B,
VERIFY THE INTEGRITY OF PUBLIC KEY CERTIFICATE OF A WITH PUBLIC KEY OF IA,
OBTAIN A.Sig.Ver.Key (PUBLIC KEY OF A),
VERIFY THE INTEGRITY OF A.Sig.WITH. A.Sig.Ver.Key,
GENERATE RANDOM NUMBER Bk (0 < Bz < p),
CALCULATE Bv = Bk x G,
CALCULATE B.Sig. = Sign(B.Sig.Gen.Key, Rb || Ra||Bv, AND
CALCULATE Bk x Av AND SET 64-BIT X COORDINATE AS SESSION KEY
SEND B.Certificate ||Rb||Ra || Bv || B.Sig
CHECK WHETHER Ra SENT BY A IS THE SAME AS Ra CREATED BY A,
VERIFY THE INTEGRITY OF PUBLIC KEY CERTIFICATE OF B WITH PUBLIC KEY OF IA,
OBTAIN B.Sig.Ver.Key (PUBLIC KEY OF B),
VERIFY THE INTEGRITY OF B.Sig. WITH B.Sig.Ver.Key, AND
CALCULATE Ak x By AND SET 64-BIT X COORDINATE AS SESSION KEY

FIG. 12

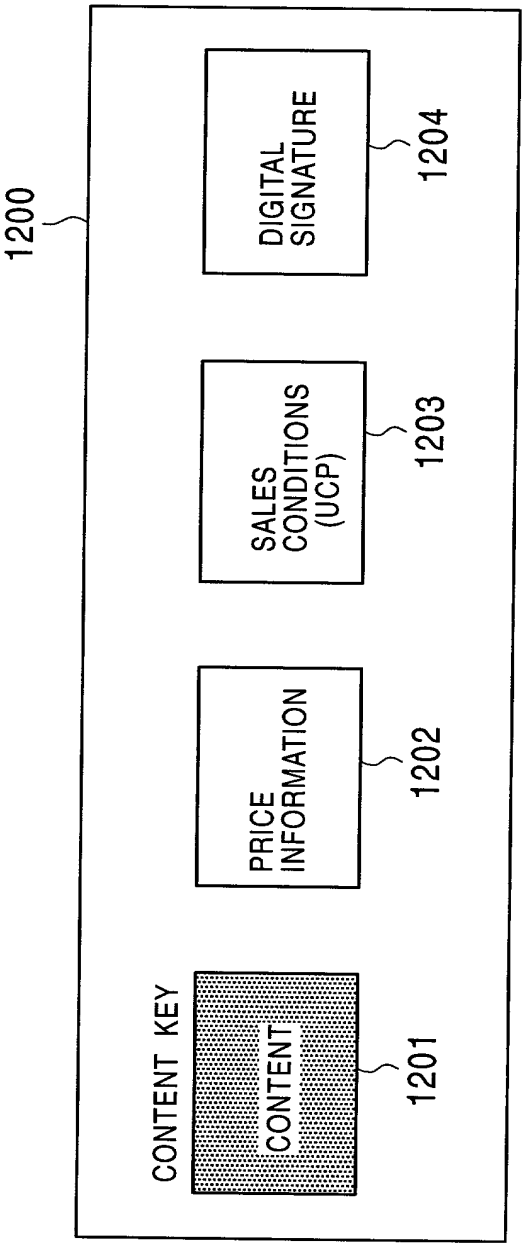

1200
CONTENT KEY
CONTENT
1201
PRICE INFORMATION
1202
SALES CONDITIONS (UCP)
1203
DIGITAL SIGNATURE
1204

FIG. 13

1301

DATA TYPE	
UCP TYPE	
UCP EFFECTIVE PERIOD	
CONTENT ID	
CONTENT PROVIDER ID	
UCP ID	
UCP VERSION	
AREA CODE	
USABLE DEVICE CONDITIONS	
USABLE USER CONDITIONS	
SERVICE PROVIDER ID	
UCP GENERATION MANAGEMENT INFORMATION	
NUMBER OF SECONDARY DELIVERIES	
NUMBER OF RULES	
RULE ADDRESS	
RULE 1	RULE NUMBER
	RIGHT-OF-USE TYPE
	RIGHT-OF-USE TYPE SALES PRICE
	CONTENT PROFIT DISTRIBUTION INFORMATION
	DATA SIZE
	:
:	:
RULE N	RULE NUMBER
	RIGHT-OF-USE TYPE
	RIGHT-OF-USE TYPE SALES PRICE
	CONTENT PROFIT DISTRIBUTION INFORMATION
	DATA SIZE
	:
(WHETHER SIGNATURE HAS BEEN VERIFIED)	
PUBLIC KEY CERTIFICATE	
SIGNATURE	

FIG. 14

1401

DATA TYPE	
PRICE INFORMATION TYPE	
PRICE INFORMATION EFFECTIVE PERIOD	
CONTENT ID	
SERVICE PROVIDER ID	
PRICE INFORMATION ID	
PRICE INFORMATION VERSION	
AREA CODE	
USABLE DEVICE CONDITIONS	
USABLE USER CONDITIONS	
CONTENT PROVIDER ID	
UCP ID	
NUMBER OF RULES	
RULE ADDRESS	
RULE 1	RULE NUMBER
	CONTENT PROFIT DISTRIUTION INFROMATION
	PRICE
	DATA SIZE
	:
:	:
RULE N	RULE NUMBER
	CONTENT PROFIT DISTRIUTION INFROMATION
	PRICE
	DATA SIZE
	:
(WHETHER SIGNATURE HAS BEEN VERIFIED)	
PUBLIC KEY CERTIFICATE	
SIGNATURE	

FIG. 15

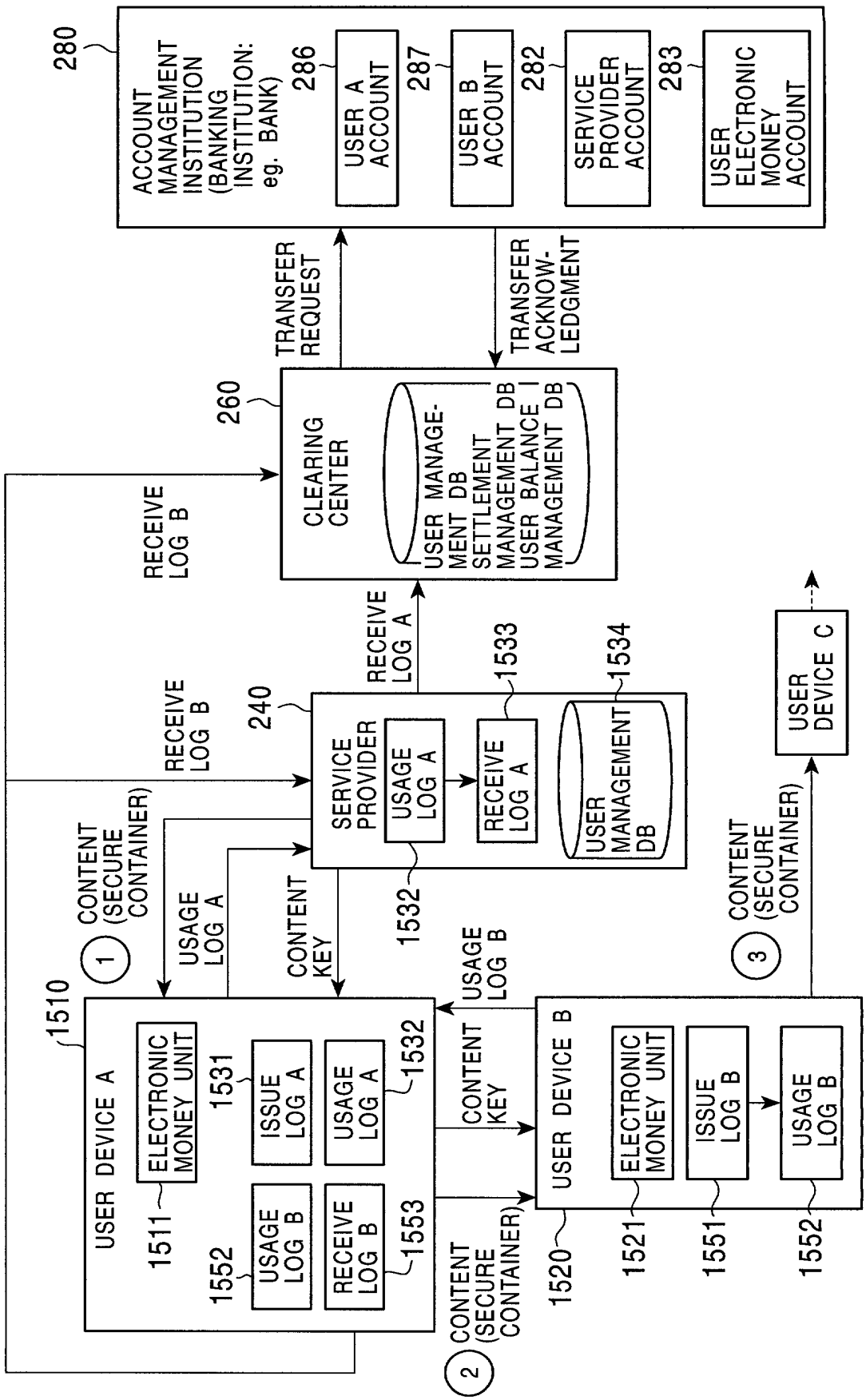

280
ACCOUNT MANAGEMENT INSTITUTION (BANKING INSTITUTION: eg. BANK)
286
USER A ACCOUNT
287
USER B ACCOUNT
282
SERVICE PROVIDER ACCOUNT
283
USER ELECTRONIC MONEY ACCOUNT
TRANSFER REQUEST
TRANSFER ACKNOW-LEDGMENT
260
CLEARING CENTER
USER MANAGE-MENT DB
SETTLEMENT MANAGEMENT DB
USER BALANCE MANAGEMENT DB
RECEIVE LOG B
RECEIVE LOG A
240
SERVICE PROVIDER
USAGE LOG A
RECEIVE LOG A
1533
1534
USER MANAGEMENT DB
USER DEVICE C
RECEIVE LOG B
CONTENT (SECURE CONTAINER)
1
USAGE LOG A
CONTENT KEY
1532
USAGE LOG B
3
CONTENT (SECURE CONTAINER)
1510
USER DEVICE A
ELECTRONIC MONEY UNIT
1511
1531
ISSUE LOG A
USAGE LOG A
1532
1552
USAGE LOG B
RECEIVE LOG B
1553
CONTENT KEY
USER DEVICE B
ELECTRONIC MONEY UNIT
ISSUE LOG B
USAGE LOG B
2
CONTENT (SECURE CONTAINER)
1520
1521
1551
1552

FIG. 16

1601

DATA TYPE
UCS TYPE
UCS EFFECTIVE PERIOD
CONTENT ID
ALBUM ID
ENCRYPTION PROCESSING UNIT ID
USER ID
CONTENT PROVIDER ID
UCP ID
UCP VERSION
SERVICE PROVIDER ID
PRICE INFORMATION ID
PRICE INFORMATION VERSION
UCS ID
RULE NUMBER OF RIGHT OF READ
RIGHT-OF-TYPE NUMBER
REMAINING NUMBER OF READS
RIGHT-OF-READ EFFECTIVE PERIOD
RULE NUMBER OF RIGHT OF COPY
RIGHT-OF-USE TYPE NUMBER
REMAINING NUMBER OF COPIES
UCS GENERATION MANAGEMENT INFORMATION
NUMBER OF UCS SECONDARY DELIVERIES
ENCRYPTION PROCESSING UNIT ID PROCESSING RIGHT OF READ

FIG. 17

1701

DATA TYPE
ENCRYPTION PROCESSING UNIT ID
USER ID (PAYER)
CONTENT ID
CONTENT PROVIDER ID
UCP ID
UCP VERSION
SERVICE PROVIDER ID
PRICE INFORMATION ID
PRICE INFORMATION VERSION
UCS ID
RULE NUMBER
PROFIT AMOUNT/PROFIT RATE OF CONTENT PROVIDER
PROFIT AMOUNT/PROFIT RATE OF SERVICE PROVIDER
PROFIT AMOUNT/PROFIT RATE OF OTHER ORGANIZATIONS
UCP GENERATION MANAGEMENT INFORMATION
SETTING INFORMATION DATA SIZE OF CONTENT PROVIDER
SETTING INFORMATION OF CONTENT PROVIDER
SETTING INFORMATION DATA SIZE OF SERVICE PROVIDER
SETTING INFORMATION OF SERVICE PROVIDER
RECEIVED DATA
SERIAL NUMBER
SUPPLIER ID

FIG. 18

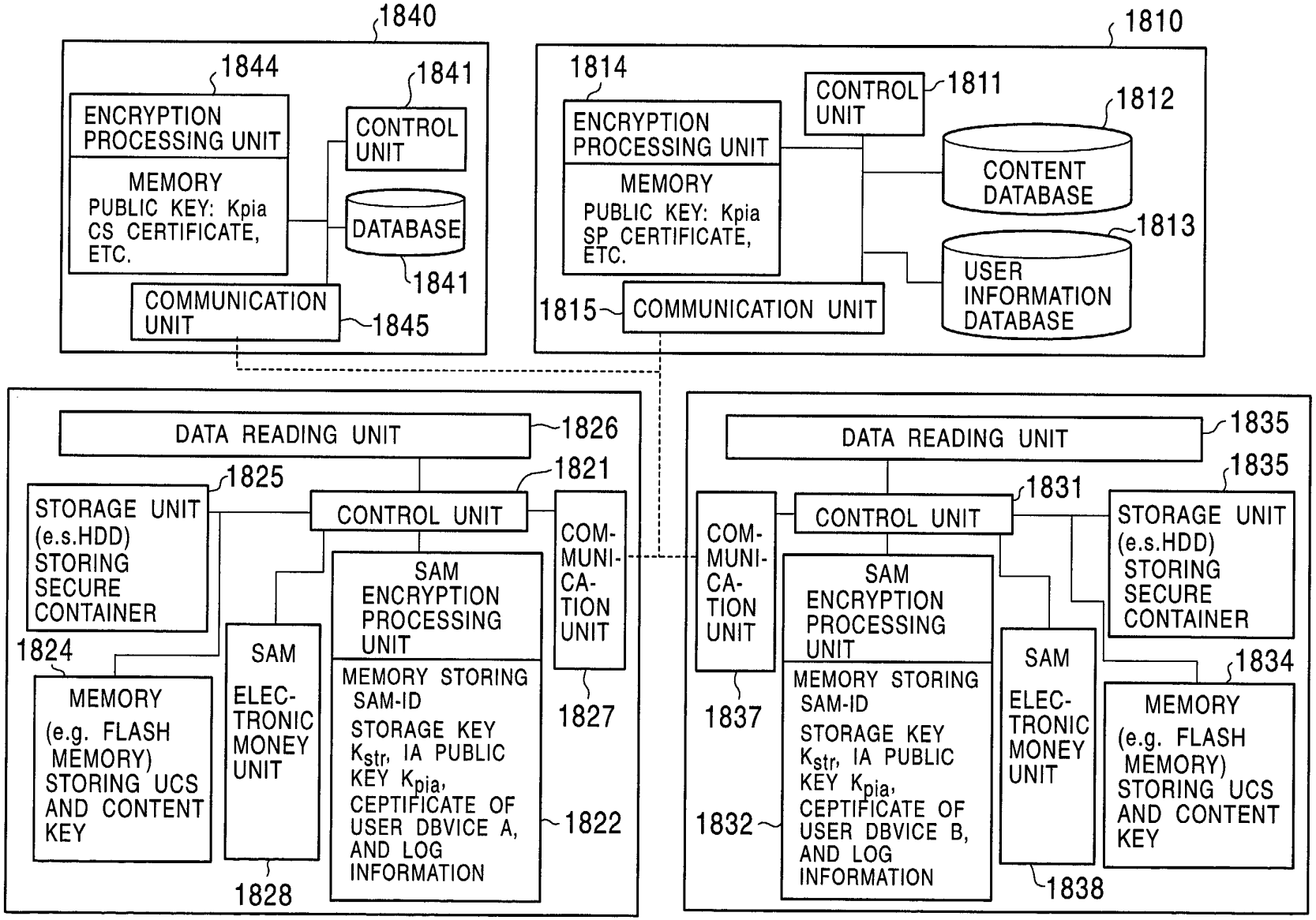

1840
1844
ENCRYPTION PROCESSING UNIT
MEMORY
PUBLIC KEY: Kpia
CS CERTIFICATE, ETC.
1841
CONTROL UNIT
DATABASE
1841
COMMUNICATION UNIT
1845
1810
1814
ENCRYPTION PROCESSING UNIT
MEMORY
PUBLIC KEY: Kpia
SP CERTIFICATE, ETC.
CONTROL UNIT
1811
1812
CONTENT DATABASE
1813
USER INFORMATION DATABASE
1815
COMMUNICATION UNIT
DATA READING UNIT
1826
1825
STORAGE UNIT (e.s.HDD) STORING SECURE CONTAINER
1821
CONTROL UNIT
COM-MUNI-CA-TION UNIT
1827
SAM ENCRYPTION PROCESSING UNIT
MEMORY STORING SAM-ID
STORAGE KEY Kstr, IA PUBLIC KEY Kpia, CEPTIFICATE OF USER DBVICE A, AND LOG INFORMATION
1822
1824
MEMORY (e.g. FLASH MEMORY) STORING UCS AND CONTENT KEY
SAM ELEC-TRONIC MONEY UNIT
1828
DATA READING UNIT
1835
1835
STORAGE UNIT (e.s.HDD) STORING SECURE CONTAINER
1831
CONTROL UNIT
COM-MUNI-CA-TION UNIT
1837
SAM ENCRYPTION PROCESSING UNIT
MEMORY STORING SAM-ID
STORAGE KEY Kstr, IA PUBLIC KEY Kpia, CEPTIFICATE OF USER DBVICE B, AND LOG INFORMATION
1832
SAM ELEC-TRONIC MONEY UNIT
1838
1834
MEMORY (e.g. FLASH MEMORY) STORING UCS AND CONTENT KEY

FIG. 19

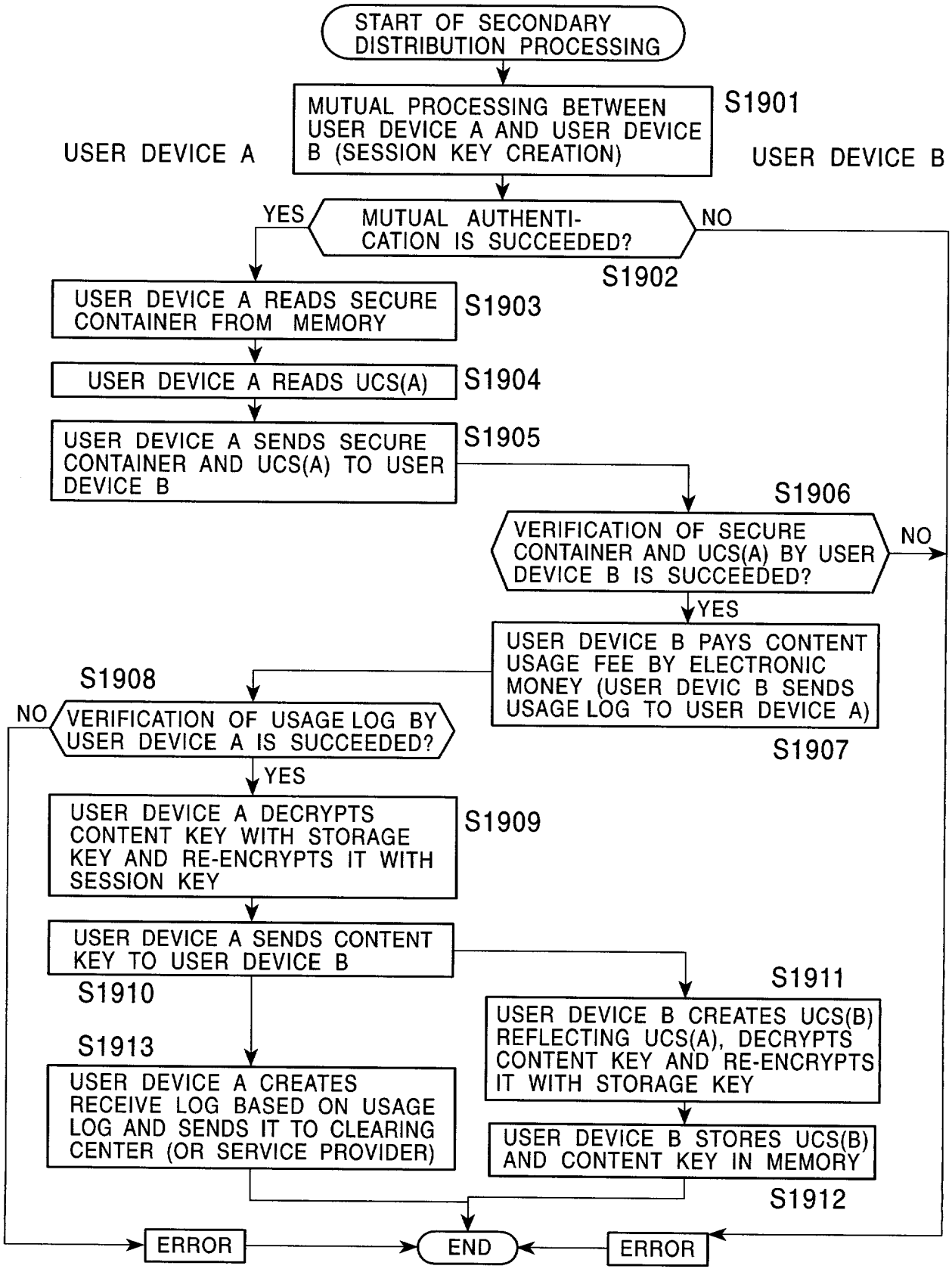

START OF SECONDARY DISTRIBUTION PROCESSING
MUTUAL PROCESSING BETWEEN USER DEVICE A AND USER DEVICE B (SESSION KEY CREATION)
S1901
USER DEVICE A
USER DEVICE B
YES
MUTUAL AUTHENTI-CATION IS SUCCEEDED?
NO
S1902
USER DEVICE A READS SECURE CONTAINER FROM MEMORY
S1903
USER DEVICE A READS UCS(A)
S1904
USER DEVICE A SENDS SECURE CONTAINER AND UCS(A) TO USER DEVICE B
S1905
S1906
VERIFICATION OF SECURE CONTAINER AND UCS(A) BY USER DEVICE B IS SUCCEEDED?
NO
YES
USER DEVICE B PAYS CONTENT USAGE FEE BY ELECTRONIC MONEY (USER DEVIC B SENDS USAGE LOG TO USER DEVICE A)
S1907
S1908
NO
VERIFICATION OF USAGE LOG BY USER DEVICE A IS SUCCEEDED?
YES
USER DEVICE A DECRYPTS CONTENT KEY WITH STORAGE KEY AND RE-ENCRYPTS IT WITH SESSION KEY
S1909
USER DEVICE A SENDS CONTENT KEY TO USER DEVICE B
S1910
S1911
USER DEVICE B CREATES UCS(B) REFLECTING UCS(A), DECRYPTS CONTENT KEY AND RE-ENCRYPTS IT WITH STORAGE KEY
S1913
USER DEVICE A CREATES RECEIVE LOG BASED ON USAGE LOG AND SENDS IT TO CLEARING CENTER (OR SERVICE PROVIDER)
USER DEVICE B STORES UCS(B) AND CONTENT KEY IN MEMORY
S1912
ERROR
END
ERROR

FIG. 20

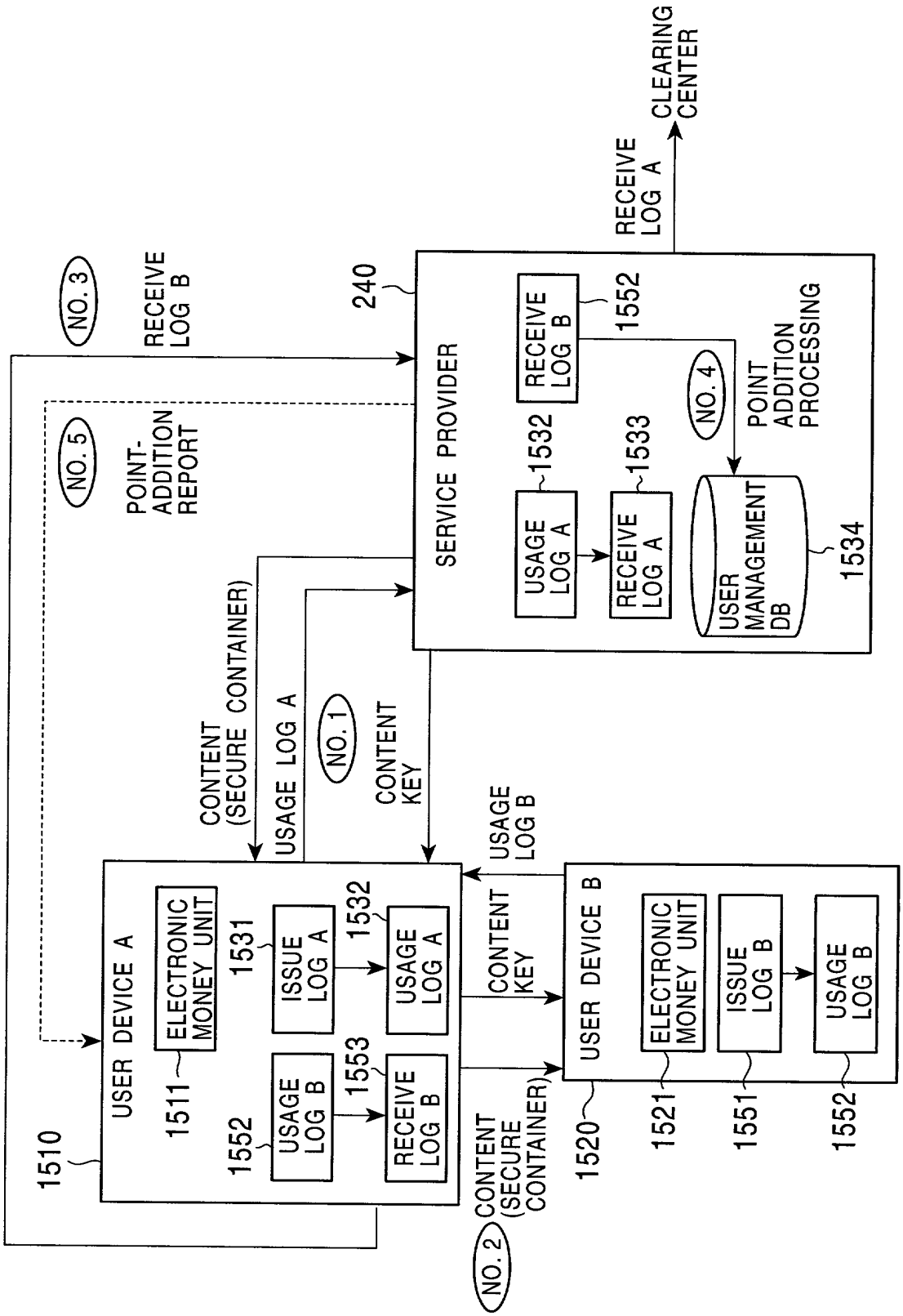

CLEARING CENTER
RECEIVE LOG A
240
SERVICE PROVIDER
RECEIVE LOG B
1552
NO. 4
POINT ADDITION PROCESSING
USAGE LOG A
1532
RECEIVE LOG A
1533
USER MANAGEMENT DB
1534
NO. 3
RECEIVE LOG B
NO. 5
POINT-ADDITION REPORT
CONTENT (SECURE CONTAINER)
USAGE LOG A
NO. 1
CONTENT KEY
USAGE LOG B
USER DEVICE A
ELECTRONIC MONEY UNIT
1511
ISSUE LOG A
1531
USAGE LOG A
1532
USAGE LOG B
1552
RECEIVE LOG B
1553
1510
CONTENT KEY
CONTENT (SECURE CONTAINER)
NO. 2
USER DEVICE B
ELECTRONIC MONEY UNIT
ISSUE LOG B
USAGE LOG B
1520
1521
1551
1552

FIG. 21

USER ID	USER DEVICE ID	CONTENT ID	RECEIVE LOG ID	POINT
ABC0001	CDE00021	AAA001	BBB001	02
ABC0002	CDE00027	B05002	BA8822	05
ABC0003	CDE03211	CC0812	BA0214	12
⋮	⋮	⋮	⋮	⋮
BBC0231	EED02333	ABD325	BAA883	07

FIG. 22

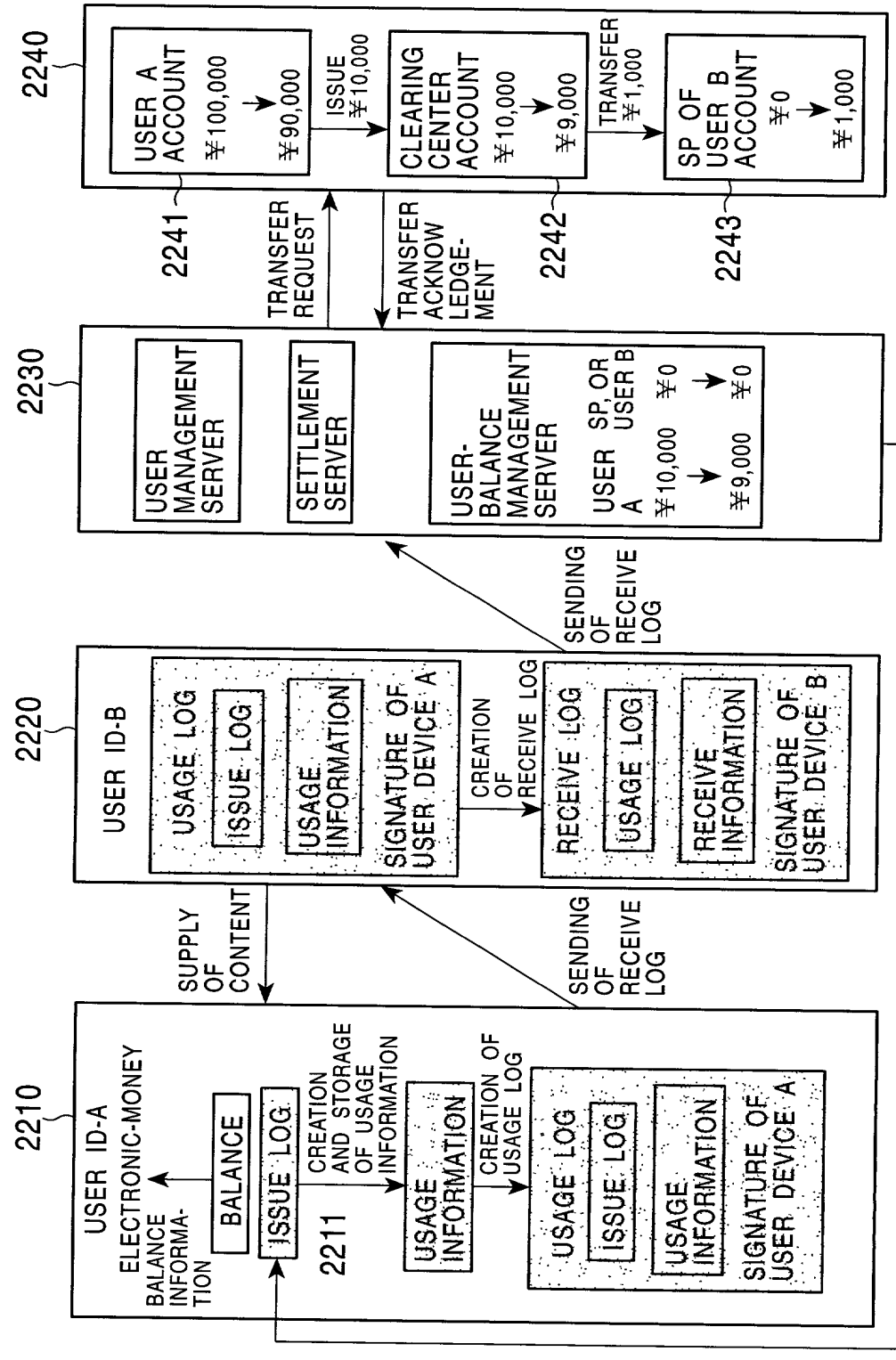

2240
USER A ACCOUNT
¥100,000
¥90,000
ISSUE ¥10,000
CLEARING CENTER ACCOUNT
¥10,000
¥9,000
TRANSFER ¥1,000
SP OF USER B ACCOUNT
¥0
¥1,000
2241
2242
2243
TRANSFER REQUEST
TRANSFER ACKNOW LEDGE-MENT
2230
USER MANAGEMENT SERVER
SETTLEMENT SERVER
USER-BALANCE MANAGEMENT SERVER
USER A
SP, OR USER B
¥10,000 ¥0
¥9,000 ¥0
SENDING OF RECEIVE LOG
2220
USER ID-B
USAGE LOG
ISSUE LOG
USAGE INFORMATION
SIGNATURE OF USER DEVICE A
CREATION OF RECEIVE LOG
RECEIVE LOG
USAGE LOG
RECEIVE INFORMATION
SIGNATURE OF USER DEVICE B
SUPPLY OF CONTENT
SENDING OF RECEIVE LOG
2210
USER ID-A
ELECTRONIC-MONEY
BALANCE INFORMA-TION
BALANCE
ISSUE LOG
2211
CREATION AND STORAGE OF USAGE INFORMATION
USAGE INFORMATION
CREATION OF USAGE LOG
USAGE LOG
ISSUE LOG
USAGE INFORMATION
SIGNATURE OF USER DEVICE A
ISSUING ELECTRONIC MONEY TO USER DEVICE A

FIG. 23

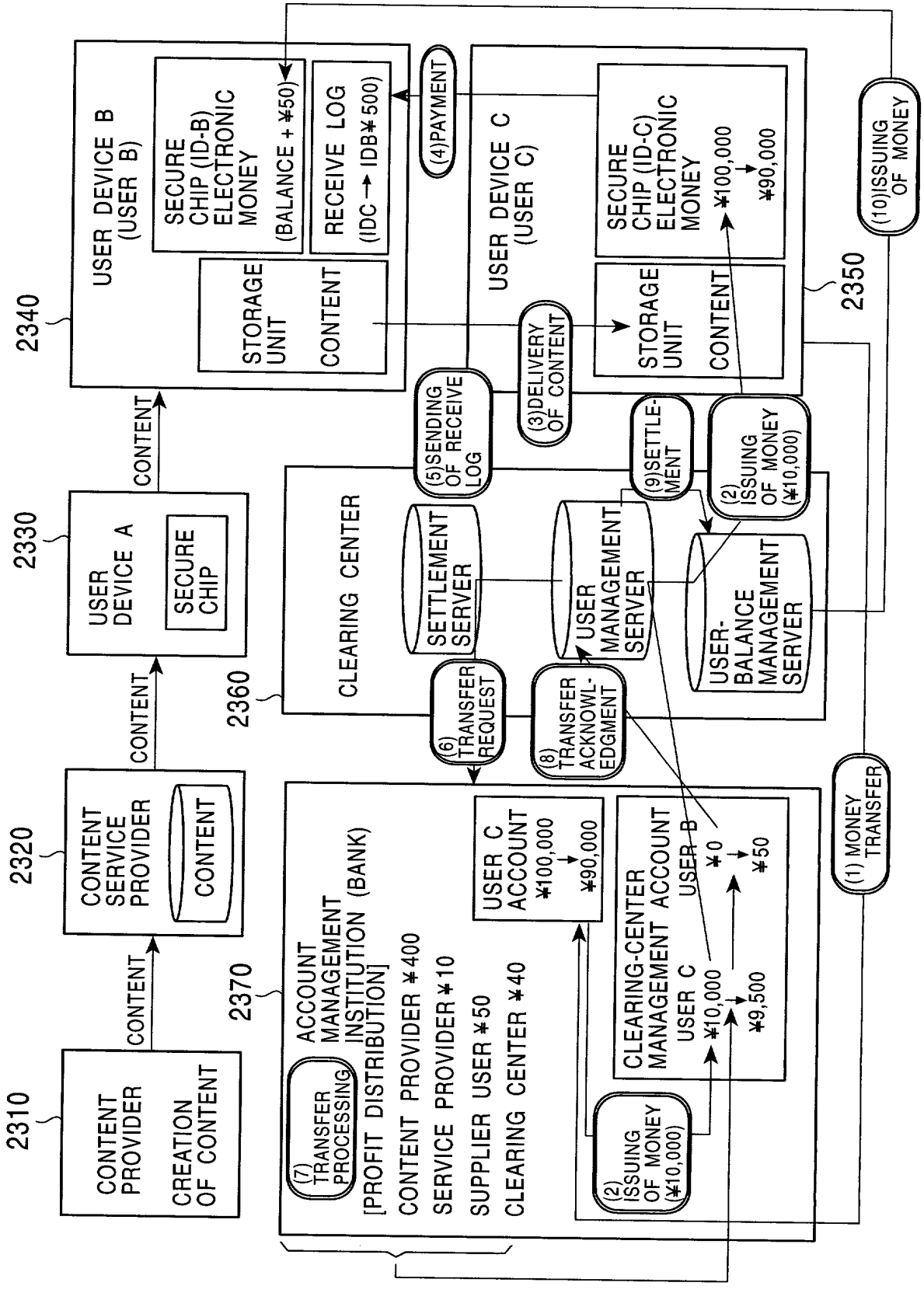

2310
CONTENT PROVIDER
CREATION OF CONTENT
CONTENT
2320
CONTENT SERVICE PROVIDER
CONTENT
CONTENT
2330
USER DEVICE A
SECURE CHIP
CONTENT
2340
USER DEVICE B (USER B)
SECURE CHIP (ID-B) ELECTRONIC MONEY
(BALANCE + ¥50)
RECEIVE LOG
(IDC → IDB ¥500)
STORAGE UNIT
CONTENT
(4)PAYMENT
USER DEVICE C (USER C)
SECURE CHIP (ID-C) ELECTRONIC MONEY
¥100,000
¥90,000
STORAGE UNIT
CONTENT
2350
(10)ISSUING OF MONEY
(1) MONEY TRANSFER
2360
CLEARING CENTER
SETTLEMENT SERVER
USER MANAGEMENT SERVER
USER-BALANCE MANAGEMENT SERVER
(5)SENDING OF RECEIVE LOG
(3)DELIVERY OF CONTENT
(9)SETTLE-MENT
(2) ISSUING OF MONEY (¥10,000)
(6) TRANSFER REQUEST
(8) TRANSFER ACKNOWL-EDGMENT
2370
ACCOUNT MANAGEMENT INSTITUTION (BANK)
[PROFIT DISTRIBUTION]
CONTENT PROVIDER ¥400
SERVICE PROVIDER ¥10
SUPPLIER USER ¥50
CLEARING CENTER ¥40
(7) TRANSFER PROCESSING
USER C ACCOUNT
¥100,000
¥90,000
CLEARING-CENTER MANAGEMENT ACCOUNT
USER C
¥10,000
¥9,500
USER B
¥0
¥50
(2) ISSUING OF MONEY (¥10,000)

FIG. 24

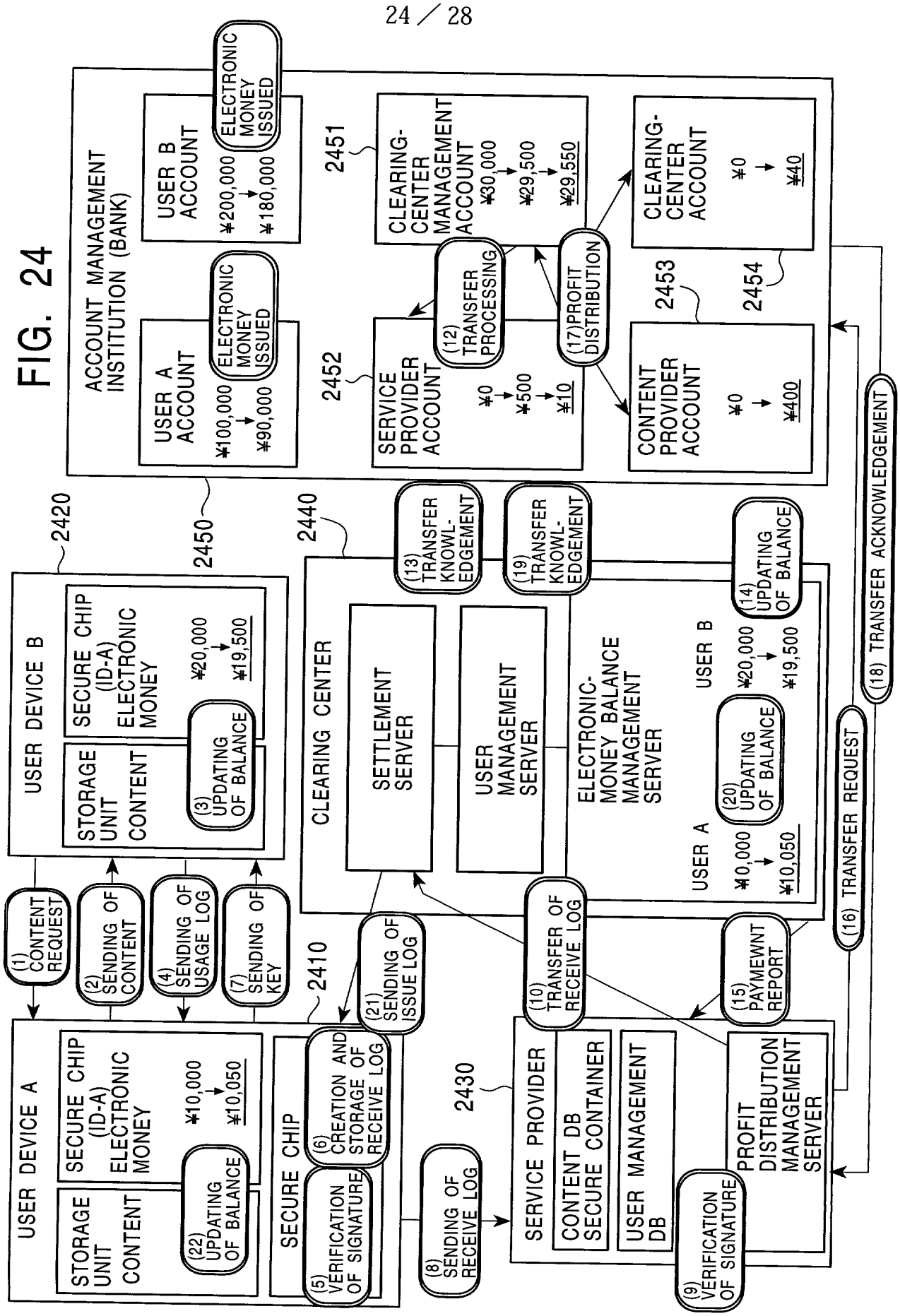
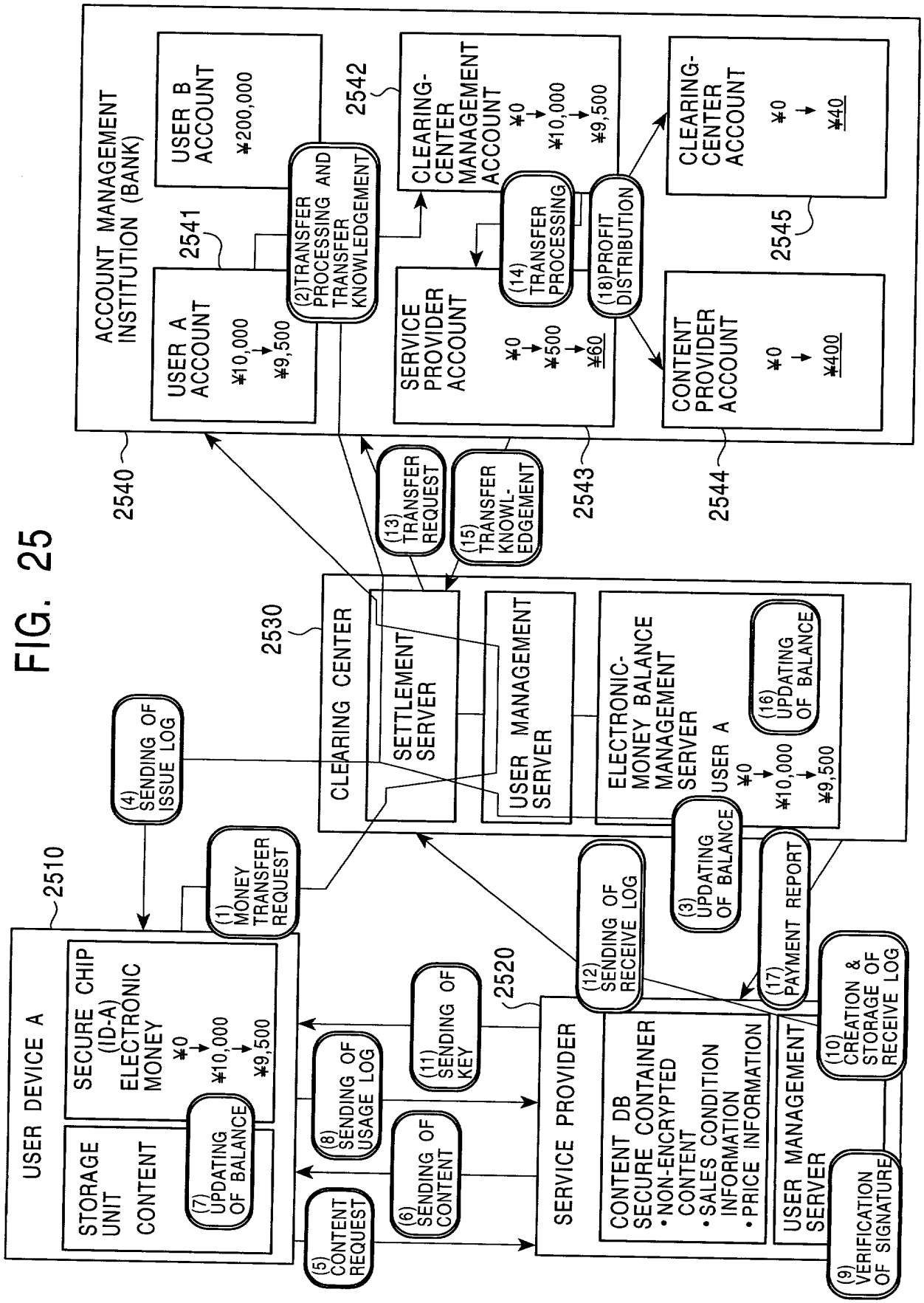

ACCOUNT MANAGEMENT INSTITUTION (BANK)
USER A ACCOUNT
¥100,000 → ¥90,000
ELECTRONIC MONEY ISSUED
USER B ACCOUNT
¥200,000 → ¥180,000
ELECTRONIC MONEY ISSUED
2451
CLEARING-CENTER MANAGEMENT ACCOUNT
¥30,000 → ¥29,500 → ¥29,550
2452
SERVICE PROVIDER ACCOUNT
¥0 → ¥500 → ¥10
(12) TRANSFER PROCESSING
(17) PROFIT DISTRIBUTION
2453
CONTENT PROVIDER ACCOUNT
¥0 → ¥400
2454
CLEARING-CENTER ACCOUNT
¥0 → ¥40
2450
2420
USER DEVICE B
STORAGE UNIT CONTENT
SECURE CHIP (ID-A) ELECTRONIC MONEY
¥20,000 → ¥19,500
(3) UPDATING OF BALANCE
2440
CLEARING CENTER
SETTLEMENT SERVER
USER MANAGEMENT SERVER
ELECTRONIC-MONEY BALANCE MANAGEMENT SERVER
(13) TRANSFER KNOWL-EDGEMENT
(19) TRANSFER KNOWL-EDGEMENT
(14) UPDATING OF BALANCE
USER B
¥20,000 → ¥19,500
(20) UPDATING OF BALANCE
USER A
¥0,000 → ¥10,050
(1) CONTENT REQUEST
(2) SENDING OF CONTENT
(4) SENDING OF USAGE LOG
(7) SENDING OF KEY
2410
USER DEVICE A
STORAGE UNIT CONTENT
SECURE CHIP (ID-A) ELECTRONIC MONEY
¥10,000 → ¥10,050
(22) UPDATING OF BALANCE
SECURE CHIP
(5) VERIFICATION OF SIGNATURE
(6) CREATION AND STORAGE OF RECEIVE LOG
(21) SENDING OF ISSUE LOG
(8) SENDING OF RECEIVE LOG
2430
SERVICE PROVIDER
CONTENT DB SECURE CONTAINER
USER MANAGEMENT DB
(10) TRANSFER OF RECEIVE LOG
(15) PAYMEWNT REPORT
PROFIT DISTRIBUTION MANAGEMENT SERVER
(9) VERIFICATION OF SIGNATURE
(16) TRANSFER REQUEST
(18) TRANSFER ACKNOWLEDGEMENT

FIG. 25


USER DEVICE A
2510
STORAGE UNIT
CONTENT
SECURE CHIP (ID-A)
ELECTRONIC MONEY
¥0
¥10,000
¥9,500
(7) UPDATING OF BALANCE
(1) MONEY TRANSFER REQUEST
(4) SENDING OF ISSUE LOG
(5) CONTENT REQUEST
(8) SENDING OF USAGE LOG
(6) SENDING OF CONTENT
(11) SENDING OF KEY
2520
SERVICE PROVIDER
CONTENT DB
SECURE CONTAINER
• NON-ENCRYPTED CONTENT
• SALES CONDITION INFORMATION
• PRICE INFORMATION
USER MANAGEMENT SERVER
(9) VERIFICATION OF SIGNATURE
(10) CREATION & STORAGE OF RECEIVE LOG
(12) SENDING OF RECEIVE LOG
2530
CLEARING CENTER
SETTLEMENT SERVER
USER MANAGEMENT SERVER
ELECTRONIC-MONEY BALANCE MANAGEMENT SERVER
USER A
¥0
¥10,000
¥9,500
(3) UPDATING OF BALANCE
(16) UPDATING OF BALANCE
(17) PAYMENT REPORT
(13) TRANSFER REQUEST
(15) TRANSFER KNOWL-EDGEMENT
2540
ACCOUNT MANAGEMENT INSTITUTION (BANK)
USER A ACCOUNT
¥10,000
¥9,500
2541
USER B ACCOUNT
¥200,000
(2) TRANSFER PROCESSING AND TRANSFER KNOWLEDGEMENT
2542
CLEARING-CENTER MANAGEMENT ACCOUNT
¥0
¥10,000
¥9,500
SERVICE PROVIDER ACCOUNT
¥0
¥500
¥60
(14) TRANSFER PROCESSING
(18) PROFIT DISTRIBUTION
2543
CONTENT PROVIDER ACCOUNT
¥0
¥400
2544
CLEARING-CENTER ACCOUNT
¥0
¥40
2545

PATENT APPLICATION

FIG. 26

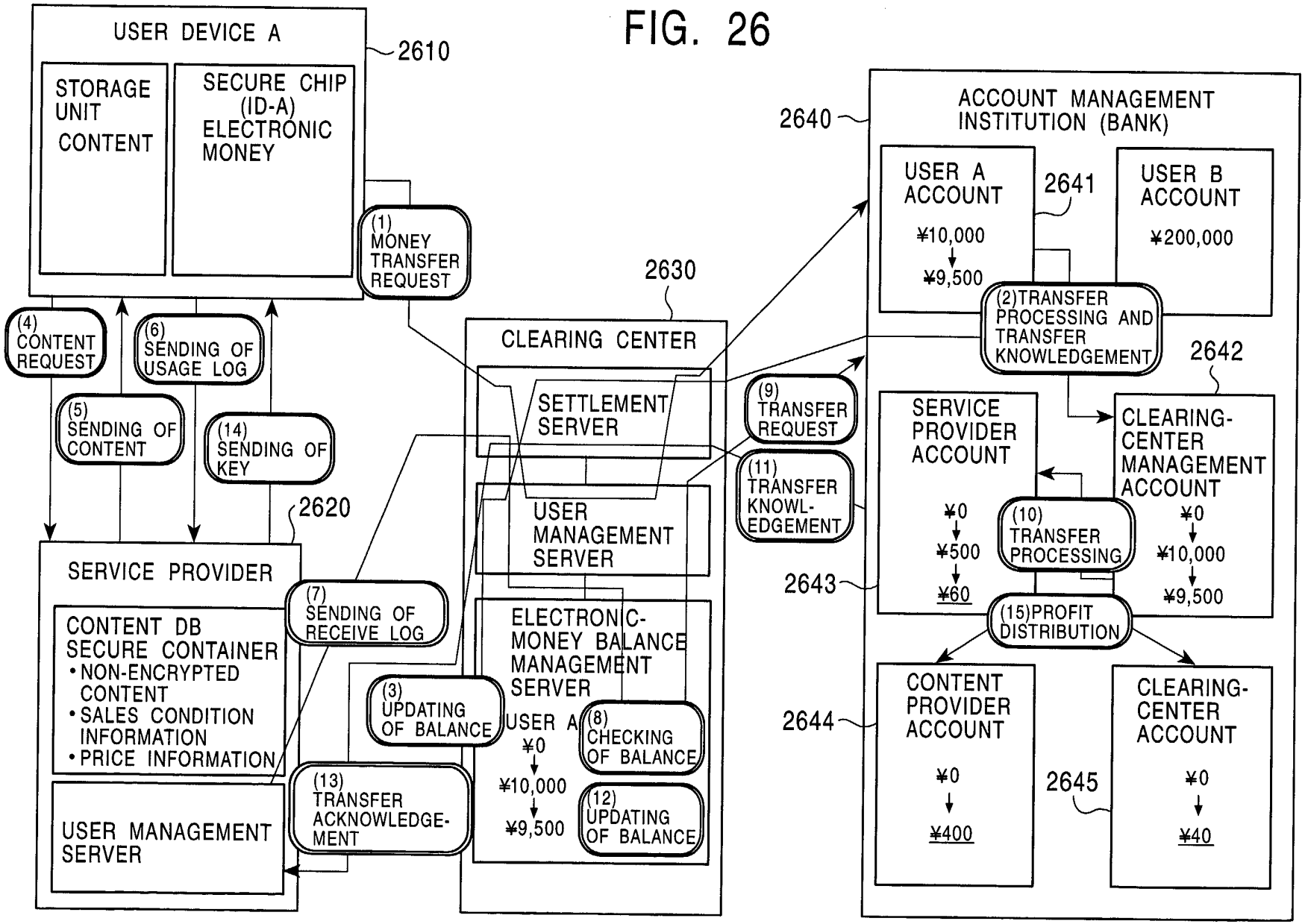


FIG. 27

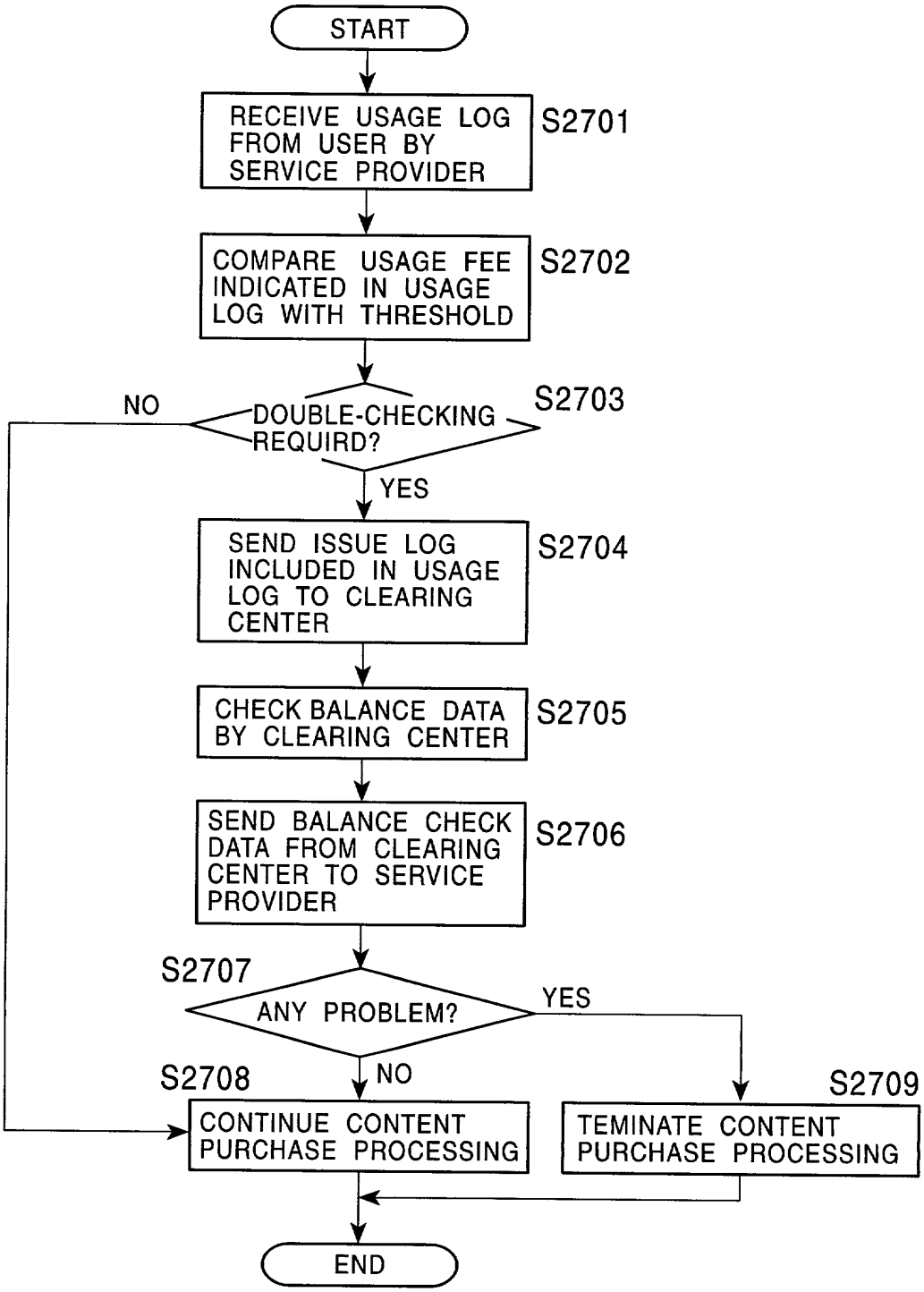
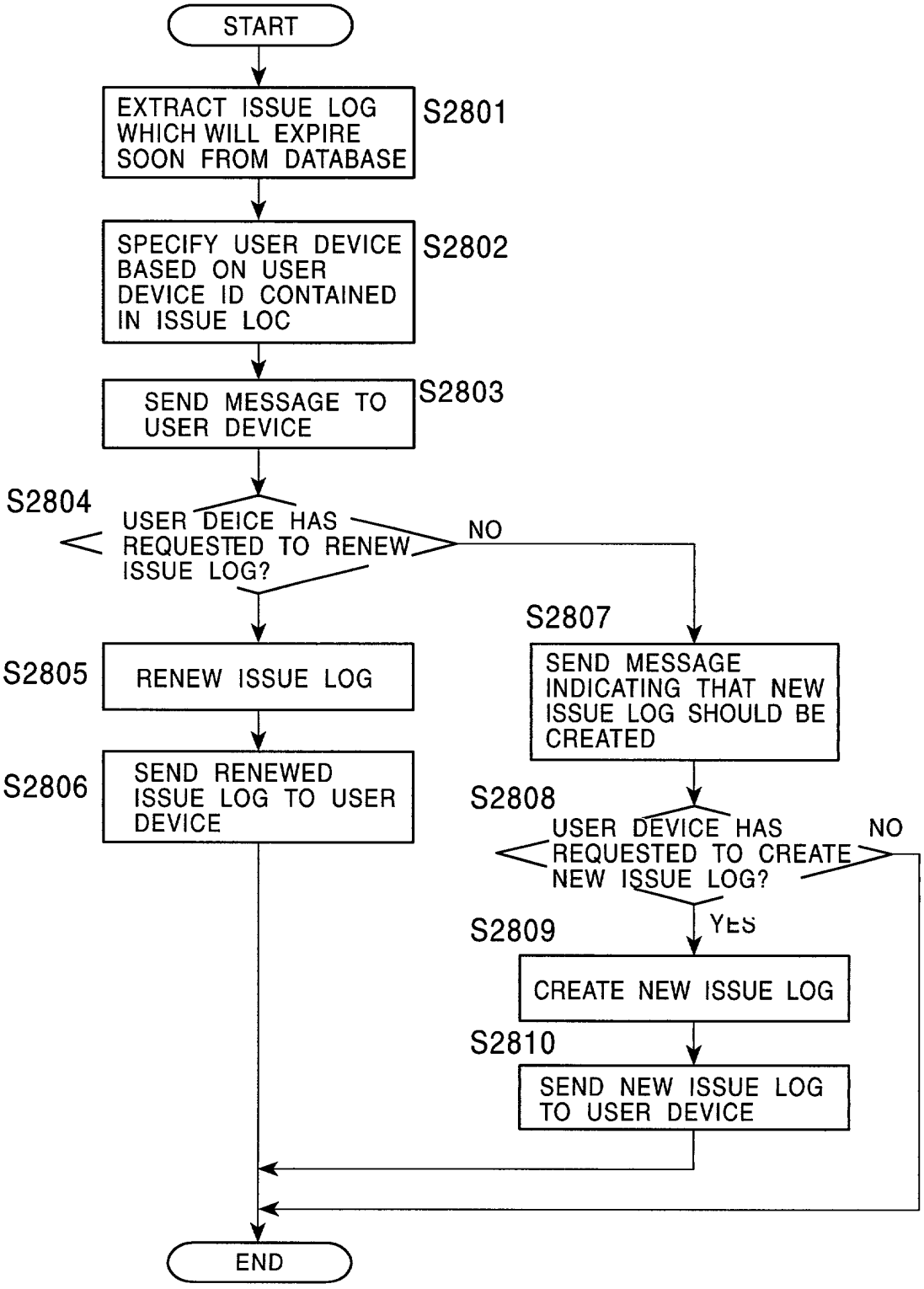

START
RECEIVE USAGE LOG FROM USER BY SERVICE PROVIDER
S2701
COMPARE USAGE FEE INDICATED IN USAGE LOG WITH THRESHOLD
S2702
DOUBLE-CHECKING REQUIRD?
S2703
NO
YES
SEND ISSUE LOG INCLUDED IN USAGE LOG TO CLEARING CENTER
S2704
CHECK BALANCE DATA BY CLEARING CENTER
S2705
SEND BALANCE CHECK DATA FROM CLEARING CENTER TO SERVICE PROVIDER
S2706
S2707
ANY PROBLEM?
YES
NO
S2708
S2709
CONTINUE CONTENT PURCHASE PROCESSING
TEMINATE CONTENT PURCHASE PROCESSING
END

FIG. 28


START
EXTRACT ISSUE LOG WHICH WILL EXPIRE SOON FROM DATABASE
S2801
SPECIFY USER DEVICE BASED ON USER DEVICE ID CONTAINED IN ISSUE LOC
S2802
SEND MESSAGE TO USER DEVICE
S2803
S2804
USER DEICE HAS REQUESTED TO RENEW ISSUE LOG?
NO
S2805
RENEW ISSUE LOG
S2806
SEND RENEWED ISSUE LOG TO USER DEVICE
S2807
SEND MESSAGE INDICATING THAT NEW ISSUE LOG SHOULD BE CREATED
S2808
USER DEVICE HAS REQUESTED TO CREATE NEW ISSUE LOG?
NO
YES
S2809
CREATE NEW ISSUE LOG
S2810
SEND NEW ISSUE LOG TO USER DEVICE
END